Year 2000 Lessons Learned:
Strategies for Successful Global Project Management

U.S. Department of State
Office of Inspector General

Report Number 01-IT-008

May 2001

"Y2K was fascinating in terms of how to get one's arms around a subtle problem that crossed a wide sweep: 180 countries, 50 states, the entire U.S. economy, and the whole U.S. Government. We will not have to do it again in the near future, however the lessons learned from the exercise will be invaluable in addressing other management issues."

— **Chair**, President's Council on Year 2000 Conversion, United States

PREFACE

The Year 2000 (Y2K) management crisis is over. For months, the world worked diligently, cooperatively, and in ways unheard of before to prepare computer systems and supporting infrastructures for the millennium date change. Ultimately, global Y2K management efforts and the financial and staff resources invested in them paid off. Despite the many negative predictions of Y2K outcomes made in advance of the rollover, we successfully passed all critical dates and transitioned into the New Year with only minimal disruptions across the globe. Numerous glitches resulting from the rollover were reportedly all relatively minor, with no lasting effects on private or public systems and infrastructures in countries worldwide.

The Y2K crisis was a unique experience, both in terms of the challenge faced and the global management strategies and activities implemented to overcome it. Given its success, we conducted a retrospective study of the global Y2K management effort to identify effective practices and lessons learned that can be adapted and applied for future benefit. We have outlined the results of our study in this report. This information is intended to provide guidance for international business and government officials to use in future efforts to address information technology (IT) or other emerging global management challenges.

This report was prepared under the direction of Frank W. Deffer, Acting Assistant Inspector General, Information Technology Issues. Other key contributors were Monique C. Austin, Sondra F. McCauley, and Christina B. Watson. If you have questions or comments concerning this report, please contact Mr. Deffer at (703) 284-2715 or defferf@state.gov. Mail may be directed to Mr. Deffer at U.S. Department of State, Office of Inspector General, Information Technology Issues, Room 930, 1700 N. Moore Street, Arlington, VA 22209.

Anne M. Sigmund
Acting Inspector General

CONTENTS

ABBREVIATIONS

HKMA	Hong Kong Monetary Authority	**IT**	information technology
***info*Dev**	Information for Development	**OIG**	Office of Inspector General
IY2KCC	International Year 2000 Cooperation Center	**UN**	United Nations
		Y2K	Year 2000

Executive Summary

Purpose

This report outlines the results of our study of leading practices, ancillary benefits, and lessons learned—both positive and negative—from the Y2K crisis management exercise. Our work is built on interviews and data gathering in the Washington, DC, metropolitan area, at financial institutions and the United Nations (UN) in New York City, at one U.S. military base, and in eight locations around the globe. Rather than an audit, the report brings together the perspectives and analysis of many key players and observers in the Y2K management exercise. This information is intended to provide guidance that managers might consider and apply in undertaking global projects to address IT or other emerging global issues in the new millennium.

Background

Rapid advancements in IT and heightened interconnectivity through use of the Internet have revolutionized the way in which much of the world communicates and conducts business operations. In the current technological environment, industries and governments worldwide have been challenged to adopt broader IT perspectives and no longer strictly manage technology in the context of their individual operations. The recent Y2K technology problem and subsequent global efforts to address it exemplified this challenge. Like no other issue before, Y2K illustrated the need for international IT cooperation to ensure that, while the world continues to reap the benefits of systems innovations, we also effectively manage the risks and vulnerabilities that increased automation brings with it.

To address the Y2K threat, countries and organizations worldwide worked together, sharing information and managing in ways unheard of before to avert potential disruptions and disasters. Finally, at midnight December 31, 1999, we made it through the millennium transition with minimal disruptions and no major impact. Based on tests conducted in advance to simulate possible Y2K impacts, and the hundreds of minor glitches reported after the rollover, we averted a very real disaster. Although there is a tendency by many to write the Y2K exercise off as a nonevent and move on to other issues, we believe it would be a mistake not to take a second look and excerpt the messages it conveyed. Y2K readiness was an excellent illustration of global project management. We have much to learn from it.

Overview of Principles and Practices for Successful Global Project Management

This report is organized into six key principles that provide a framework for discussing successful practices and lessons we identified from our Y2K review. The six principles are:

I. Recognize Leadership and Commitment as Keys to Success
II. Appreciate the Value of Coordination, Cooperation, and Collaboration
III. Exploit Opportunities for Management Improvements
IV. Coordinate Guidance, Monitoring, and Data Reporting and Analysis Activities
V. Build Public Awareness and Confidence
VI. Consider Cultural Differences

We have grouped these principles into three overarching categories that summarize at the highest level the essence of all the individual practices and lessons we gleaned from Y2K management. Each of these groupings is discussed below.

Organizational Relationships

We have coupled Principles I and II into the category of "Organizational Relationships," because they concern how projects are governed and supported from the top down and how key players in the global project can interact and support one another in accomplishing their mutual objectives. Practices in the area of governing global projects include understanding the U.S. leadership responsibility for addressing international issues, optimizing the contribution of key individuals in rallying worldwide cooperation, and ensuring involvement by senior managers to provide the resources, focus, and effort needed for successful global project management. Practices concerning organizational interaction include promoting shared responsibility for tackling common issues at the global, regional, sector, and national levels. They also include recognizing the benefits and necessity for government/industry partnerships and legal/regulatory support in addressing worldwide management challenges.

Information and Technology Management

Principles III and IV are categorized together under the single heading of "Information and Technology Management." These principles deal with tangible assets and practical matters—systems and equipment, data and processes—and how their management can be improved during a project. Specifically, some side benefits of the Y2K project include greater recognition of the importance of IT to mission accomplishment, increased contingency planning and emergency preparedness, and effective use of innovative IT tools and techniques. The Y2K exercise also demonstrated the need for global project managers to provide clear guidance to field offices, reduce duplicative data collection activities, eliminate redundant and burdensome reporting requirements, synthesize data analysis, and coordinate status monitoring and communications activities. Further, Y2K emphasized the proactive role that audit organizations can play in management problem resolution.

Human Relations

Finally, Principles V and VI deal with people-related matters that we have placed under the heading of "Human Relations." For instance, the Y2K experience demonstrated that managing fear, launching public awareness campaigns, and instituting emergency safeguards are critical aspects of gaining individual support and cooperation in overcoming a global threat. Y2K also illustrated the need for the United States and other industrialized nations to look beyond Western perspectives and recognize the different needs, approaches, and views of other nations and cultures in global project management.

Taken together, the three overarching categories highlight the principal areas of focus for ensuring successful global project management. We discuss each principle and corresponding practices in this report, along with actual examples and case study illustrations of selected practices. **Table 1** illustrates how we have organized the principles and practices for ensuring successful global project management into the three overarching categories. This table is intended to serve as a composite guide for the reader of this report and facilitate understanding of the subsequent discussions of the six principles and detailed practices that they encompass.

We recognize that this framework as a whole may not be suitable for all issues or organizations. We nonetheless believe that, at the very least, some subset of the principles and individual practices discussed can be considered, adapted, and applied as appropriate to benefit the Department, the nation, and the world in addressing IT and other global issues. Specifically, examining the leadership, management approaches, and perspectives exhibited in preparation for the Y2K date change may be helpful in addressing global IT issues such as computer security, critical infrastructure protection, Internet governance, and the digital divide as we move forward with managing information and technology in the new millennium. Effective practices and lessons learned from Y2K management may also be beneficial in undertaking other projects to address issues such as global warming or acquired immune deficiency syndrome that also pose major threats to nations across the globe.

ORGANIZATIONAL RELATIONSHIPS	INFORMATION AND TECHNOLOGY MANAGEMENT	HUMAN RELATIONS
PRINCIPLE I: Recognize Leadership and Commitment as Keys to Success	**PRINCIPLE III:** Exploit Opportunities for Management Improvements	**PRINCIPLE V:** Build Public Awareness and Confidence
PRACTICES: A. Understand the U.S. leadership role B. Optimize the contribution of key individuals C. Ensure senior-level involvement D. Provide adequate funding and commitment	PRACTICES: A. Recognize the importance of IT to business/mission accomplishment B. Be aware of the risks accompanying technological advancement C. Take advantage of opportunities to examine and improve business processes D. Improve systems management E. Emphasize systems testing and verification F. Enhance IT project management practices G. Recognize the importance of contingency planning and emergency preparedness H. Make innovative use of IT tools and techniques	PRACTICES: A. Manage fear B. Launch public awareness campaigns C. Institute public safeguards
PRINCIPLE II: Appreciate the Value of Coordination, Cooperation, and Collaboration	**PRINCIPLE IV**: Coordinate Guidance, Monitoring, and Data Reporting and Analysis Activities	**PRINCIPLE VI:** Consider Cultural Differences
PRACTICES: A. Promote worldwide cooperation at all levels B. Form public/private partnerships C. Ensure legal and regulatory support	PRACTICES: A. Effectively support decentralized crisis management activities B. Improve guidance for field operations C. Eliminate redundant and burdensome reporting requirements D. Consolidate data collection activities overseas E. Synthesize analysis of data collected F. Coordinate monitoring and communications activities G. Make proactive use of audit organizations	PRACTICES: A. Look beyond Western perspectives and approaches B. Avoid misinterpretations of foreign approaches

Table 1: Overview of Principles and Practices for Ensuring Successful Global Project Management

Background on Y2K

Y2K management was a clearly defined but highly complex problem. It was rooted in the way that many computer systems were designed to record and compute dates. Specifically, to conserve electronic data storage and reduce operating costs, computers typically used two digits to represent the year. The two-digit format, however, made the year 2000 indistinguishable from the year 1900. Using the two-digit format to perform date-sensitive calculations after 1999 could generate incorrect results. Rendering computers Y2K compliant required identifying, fixing, and testing millions of hardware systems, software applications, and data exchanges across the globe. Given the degree of reliance on automation in this modern age, the amount of remedial work to be done was daunting.

The Y2K crisis presented a unique situation—perhaps the greatest management challenge the world has ever faced. It posed a common threat, affecting governments, industry sectors, and organizations of all types and sizes everywhere. It even touched our individual lives. It required global cooperation and collaboration to overcome. Although nations are accustomed to rallying together to address shared political or military threats, Y2K was essentially a mission and business operations problem that was rooted in technology, too. The extent and nature of potential Y2K impact on those operations remained uncertain. Y2K management also had a fixed deadline; there was zero tolerance for failure. Inability to address the Y2K issue by the deadline could have widespread and potentially disastrous implications. The high degree of systems integration and interdependencies in the current era further complicated matters, making multiple, simultaneous, or cascading effects highly likely.

> "It was not by chance that there were no Y2K problems. Immunization costs a lot and hard work had to happen to have a boring transition."
>
> — A National Y2K Commission official, Mexico City

Spurred by doomsday predictions[1] and widespread speculation of what might happen at the Y2K date change, nations worldwide stepped up to the challenge of ensuring that critical computer systems, infrastructures, and mission operations would remain unaffected as we entered the new millennium. Western nations—key among them the United States—led the charge. For months in advance of the deadline, governments and businesses labored individually and collectively to promote awareness, establish project management structures, remediate and test systems, monitor readiness activities, and develop contingency and emergency management plans in preparation for the date code change. They worked together, sharing tools and information in ways never imagined before. Technology—the root cause of the Y2K crisis itself—facilitated the worldwide collaboration and communication.

[1] Doomsday predictions of possible nuclear holocaust, economic recession, or multiple widespread disasters due to Y2K-related systems failures, came from a range of sources, including the press, public and private analysts, web sites, and religious groups.

But Y2K management progress did not occur without difficulty. The readiness work was hampered by obstacles that had to be dealt with—procrastination and disbelief of the need for action, misperceptions and steep learning curves, rumors and fears of the unknown, legal concerns, and financial battles for scarce resources. To many, Y2K looked too colossal and too complex to successfully resolve. Tremendous effort and resources were expended and great strides were taken to overcome the hurdles and finish by the deadline.

The whole world watched closely and breathed a sigh of relief as the New Year finally dawned in successive time zones across the globe. Contrary to the many negative projections and disaster scenarios of the preceding years, the rollover was accomplished with generally only minor systems glitches reported worldwide—i.e., automated teller machines that would not work, credit cards that could not be processed, and dates that printed out incorrectly. Apart from a few notable problems, such as a few U.S. Department of Defense satellite systems failures and several Medicare claims rejections, there was little or no impact on government operations, business functions, or our day-to-day lives. Leap-day February 29, 2000, another purportedly critical date, passed with even less impact. With each passing day of the new year, Y2K program offices shut down, focus shifted, and the world returned to business as usual, leaving the pressures and the hectic pace of Y2K preparation far behind.

In the wake of the Y2K crisis, questions remain as to what really happened during preparation for and passage of the millennium rollover. Was Y2K always destined to be a nonevent, or were the resources and efforts expended responsible for the outcome? Many simulation tests certainly demonstrated the need to prepare in advance to avert a crisis. Further, reports of hundreds of minor Y2K-related disruptions that actually occurred worldwide also provide evidence of a real problem. There are also indications that many glitches went unreported in the absence of incentives to make such information known.

In light of this evidence, one can conclude that the Y2K impact could have been much worse if steps had not been taken to remediate critical systems and processes in advance. Stopgap measures such as grounding airplanes at midnight, workarounds like resetting computer clocks, and temporarily shifting to manual or paper processes helped lighten work loads and minimize the potential for disruptions, too. Though we will never know the full story behind what happened at the Y2K rollover, the bottom line is that the world successfully accomplished what it set out to do—avoid massive Y2K-related disruptions and disasters as we entered the Year 2000.

Why Study Y2K Management Lessons Learned?

Even though probing the reason for the relatively smooth Y2K transition may be futile, examining the efforts and activities devoted to preparing for the date change can prove extremely worthwhile. As previously stated, we believe that the Y2K readiness effort provides an excellent illustration of global project management. The following are some benefits that we believe are possible as a result of conducting a retrospective study of the worldwide Y2K crisis management exercise.

Insight into Y2K preparation activities and resulting outcomes:

Retrospective study provides the opportunity to shed light on what happened during the Y2K exercise, capturing real life examples and case studies of how government and business organizations worldwide prepared for and transitioned to the new millennium. This information counters the tendency of many to write the Y2K experience off as wasted effort or a nonevent.

Illumination of Y2K successes:

Y2K management set a new standard for business and government operations at the local, national, and international levels. Never before has the world demonstrated such sharing and cooperation as it did during Y2K preparations. New concepts and innovative ways of operating were introduced. More effective ways of managing were practiced and emphasized. Though the crisis period has passed, it would be a great waste to return to former ways of operating and set aside the discipline, rigor, and creativity that Y2K imposed on management operations worldwide.

Learning from Y2K management mistakes:

Officials worldwide acknowledge that some areas of global Y2K management could have been improved. These areas include data collection and reporting, cultural awareness, and information disclosure. Examining and learning from these shortcomings can help ensure that they are not repeated in the future.

Documentation of Y2K management activities:

Given the hectic pace, ad hoc nature, and informality with which Y2K activities were often managed, much of the information from the Y2K exercise is anecdotal and was never written down. After the rollover, especially when no major disruptions occurred, many officials tended to put the Y2K situation behind them and discard their files, leaving few records of their effort. Retrospective study was essential to capturing and recording firsthand accounts of what happened during the Y2K experience before program offices were fully dismantled, key players moved on, and the information was completely lost.

> "Y2K was overestimated [but] the management lessons from it were highly underestimated."
>
> — **Former Chair**, Working Group on Informatics, United Nations

Guidance for addressing other global IT, crisis, or management issues:

Effective practices and lessons learned from the Y2K exercise can be adapted and applied to managing other emerging IT issues, including computer security, critical infrastructure protection, Internet governance, and the digital divide. The Y2K management experience can also be considered in addressing other nontechnical, worldwide threats such as global warming or acquired immune deficiency syndrome.

Objectives, Scope, and Methodology

During 1998 and 1999, the Office of Inspector General (OIG) was an effective partner with the Department of State in meeting the management challenges that the Y2K technology problem posed for critical infrastructures worldwide and their ability to continue to operate without failure into the New Year. Following the successful Y2K transition, OIG began a study to determine what effective practices and lessons could be derived from the global project management experience. With our study and this subsequent report, we sought to ensure that reaping the benefits possible from examining the Y2K experience would not remain a missed opportunity. Reports by a number of other organizations that also discuss leading practices, benefits, and lessons from Y2K management are listed in *Appendix A*.

Specific objectives of our Y2K study were to:

(1) identify management practices that were key to the success of Department of State and international Y2K programs,

(2) develop noteworthy case study examples of how these practices were carried out domestically and overseas, and

(3) determine how effective practices and lessons learned from Y2K can be used to help managers address other emerging global IT management issues.

We built our study on our efforts from March 1998 to January 2000 to monitor progress made by the Department of State and organizations worldwide in making critical systems compliant to meet the millennium date change. We began our study by examining prior work papers and sending e-mail messages to U.S. embassy and consular contacts made during our recent monitoring effort to request their initial assessments of the Y2K project and its outcome. We also conducted extensive Internet research to locate reports, articles, and other documents that discuss effective practices and lessons learned from the Y2K management exercise. Using this information, we designed our data collection approach, which included focused interviews, illustrative case studies, and documentary analysis, but no direct observation. We also developed a series of open-ended questions and discussion topics to facilitate our interviews.

"Even though we are not government leaders, we could be just as fundamental or even more so in our thinking. We can perform good work and prevent last year's work from being wasted."

— Regional Coordinator for South America and President of the Council of Government Internal Auditors, Santiago, Chile

We used these questions to obtain perspectives from a range of senior executives, project managers, and IT professionals in the local area on how they managed the Y2K effort and what could have been improved. We identified officials for interview based on points of contact established through our previous monitoring effort and recommendations from the interlocutors themselves. Officials interviewed were representatives of the Department of State and other Federal, private sector, and international organizations that had firsthand involvement in the global Y2K planning and management exercise. We also traveled to a military base to meet with Department of Defense officials about their regional Y2K activities and to New York City to meet with banking and United Nations officials that played a central role in international Y2K cooperation.

Further, we visited major cities in eight foreign locations to obtain overseas perspectives on Y2K management, outcomes, and lessons learned. We selected Chile, Egypt, England, Hong Kong, Italy, Japan, Mexico, and Singapore based on our prior visits and the willingness of Y2K officials to share information. To the extent possible, we sought to include a mix of industrialized and developing nations, and to cover a range of regions and continents. The map at **Figure 1** plots the locations that we visited as part of our overall study. At each site, we met with a variety of U.S. embassy or consulate officials responsible for ensuring and reporting on the Y2K readiness of their mission systems and facilities and for monitoring the Y2K status and activities of their host nations. We also met with a range of host country government and industry officials responsible for Y2K readiness, including national Y2K coordinators, sector representatives, trade association officials, and consultants. Where possible, we held discussions with Y2K representatives from multinational corporations and international institutions located in the cities visited.

At these locations, we relied on the officials interviewed to discuss their roles in Y2K management, their thoughts on successful practices and lessons learned from the exercise, and their ideas for applying these practices and lessons to other global management projects in the future. We did not verify the accuracy of their statements. However, where possible, we obtained reports and other materials to provide supporting documentation of their organizations' Y2K management programs, outcomes, and follow-up assessments.

We compared the data gathered from our domestic and international visits to identify successful Y2K practices, approaches, and lessons that were commonly used by organizations to manage the Y2K problem. We consolidated and refined this information into key principles that provide a framework for this report. We used noteworthy examples and case studies of successful Y2K management activities of individual organizations to illustrate how the practices were carried out in real life. Several key issues for which this guidance may be considered, adapted, and applied are discussed in the final section of this report.

We requested comments on a draft of this report from each key official or organization that participated in our review. We believed this to be the most efficient means of obtaining collective input and validation of our treatment of effective Y2K management practices and case study examples cited in the report. We have incorporated their comments and suggested changes where appropriate.

We conducted our work at the domestic and international locations listed in *Appendix B* from March through November 2000.

Figure 1: Locations Visited for Study of Successful Global Project Management Practices

Principle I: Recognize Leadership and Commitment as Keys to Success

The Y2K exercise was an excellent demonstration of the role that strong leadership and commitment play in ensuring successful global project management. Given its political and economic standing among world nations, much of the leadership for ensuring Y2K readiness came from the United States. But U.S. influence was not the only driving force in rousing nations to overcome the Y2K management challenge. The initiative and contribution of several key individuals, rising to the fore to help set direction, mobilize resources, and otherwise champion the Y2K cause, were also critical. The support and involvement of senior officials in ensuring Y2K readiness in their individual government and business organizations served as building blocks to Y2K success at the higher levels. Although financial support was a good indicator of leadership commitment to addressing the global threat, dedicated time, attention, and staff resources were just as key.

"[Y2K was] successful because the right level of people were involved — [Y2K] needed high-level people with the ability to commit resources."

— **Staff Director for Management**, Board of Governors of the Federal Reserve System, United States

Understand the U.S. Leadership Role

U.S. leadership in identifying the Y2K problem, providing funding, and assigning a focal point for the issue resulted in the opening of a number of doors.

— **Former Chair**, Working Group on Informatics, United Nations

The Y2K experience exemplified the leadership role that industrialized nations—particularly the United States—play in ensuring successful global project management. Officials worldwide told us that although international organizations are good at policymaking, only major nations have the resources or power to actually "fix things." They concluded that U.S. leadership is vital for any international cooperation effort to succeed and that this certainly held true in the case of Y2K project management.

Officials explained that, given its world standing, the United States could not help but serve in a prominent capacity in ensuring international Y2K readiness. Comprising a dominant share of the world's technology resources, much of the solution for the Y2K problem rested with the United States. Heavily reliant on technology, U.S. organizations faced just as much if not more Y2K risk than other nations in ensuring that its critical systems and processes would continue to operate uninterrupted into the new millennium. Even while expending tremendous effort and resources on Y2K readiness within its own borders, the United States also had a vested interest in also getting international Y2K efforts "right." As a major world power, the United States provided Y2K leadership through organizations such as the President's Council on Year 2000 Conversion and the International Y2K Cooperation Center (IY2KCC). As a major benefactor, this country provided international financial support for Y2K through the United Nations and the World Bank. The United States shared the responsibility with other industrialized nations, notably the "G8" nations, which also served as leaders in global Y2K management efforts.[2] U.S. Federal agencies further promoted overseas Y2K readiness through

[2] The G8 nations are Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States.

myriad conferences and sharing of tools, training, and information worldwide. U.S. corporations provided leadership for ensuring overseas Y2K readiness through forums such as Global 2000, formed to coordinate Y2K readiness among financial sector organizations, or international entities such as the International Maritime Organization or the International Civil Aviation Organization.

In turn, many foreign nations looked to the United States for leadership in Y2K management. They relied on U.S. guidance, tools, and expertise for systems remediation. They adopted the five-phased readiness approach recommended by the United States,[3] tailoring it to fit their own countries. Like the United States, they used the media to build public awareness of the Y2K problem. Some nations collaborated with the United States, working side-by-side as a team, recognizing that even as they relied on the United States, they could also cooperate by putting their own resources to use to help solve their individual problems. The head of Singapore's national Y2K task force expressed appreciation for the leadership that the United States provided to help other countries manage the Y2K problem. This official also noted that some good Y2K management guidance from U.S. sources was available on the Internet.

Optimize the Contribution of Key Individuals

Several champions emerged from the Y2K event.

— **Director, Year 2000 Enterprise Project Office, a financial institution, and Representative of the Global 2000 Coordinating Group**, New York City

As a corollary to national leadership, key individuals—by virtue of their diligence, personalities, or management approaches—can also be driving influences in accomplishing global IT management objectives. In the case of Y2K, a number of individuals from the United States and other nations played prominent roles in promoting readiness at the global, national, or regional levels. Foremost among these was John Koskinen, Chair of the President's Council on Year 2000 Conversion, United States of America.

Officials we interviewed readily identified Mr. Koskinen as the single, most significant contributor to Y2K success. Recognizing Y2K as principally a management problem as opposed to an IT problem, the President appointed Mr. Koskinen to deal with the project as such. Officials believed that he was "the right man for the job," bringing a combination of public and private experience to bear. He had a deliberate, prioritized approach, drawing upon every resource available to manage the crisis. Mr. Koskinen set out to gain the support of executive-level officials who could commit their agencies to action. He attended cabinet-level meetings, worked effectively with the Hill, and also consulted with a board of private sector executives that cut across various critical sectors. He was able to make things happen just by his leadership. He had a very small staff. Instead of trying to do everything himself, he delegated and mobilized resources, bringing together the work of the IY2KCC, the International Interagency Y2K Working Group, regulatory centers, state and local governments, intergovernmental

[3] The five phases recommended for ensuring Y2K readiness—awareness, assessment, renovation, validation, and implementation—are outlined in *Year 2000 Computing Crisis: An Assessment Guide*, U.S. General Accounting Office (GAO/AIMD-10.1.14, September 1997).

organizations, and multinational corporations to provide Y2K solutions. He showed keen political vision in marshalling U.S. resources to bring the United Nations into the Y2K effort. Through two global meetings at the United Nations, he was able to reach out to international counterparts.

Officials said that throughout the crisis, Mr. Koskinen was a calming influence—challenging the critics and managing the alarmists. Recognizing the value of public information, he held the basic view that publicly available reports were accurate and that it was not in anyone's interest to deceive and be found out later. Unlike many, he had the analysis of global Y2K readiness correct all along. When it was all over, he attributed the Y2K outcome to the work done to stop potential problems from happening. Officials suggested that the Y2K outcome could have been very different without Mr. Koskinen's influence. He saw the crisis through to the end and was successful. No one that we met with criticized him, except to regret that he had not been appointed sooner. Officials concluded that Mr. Koskinen's leadership should serve as a model for managing government/private sector interaction to address global problems in the future.

Officials with whom we met also cited a number of other key individuals for their role in achieving Y2K management success. They believed that it would be remiss not to acknowledge the contributions of these individuals in a retrospective look at Y2K. The individuals cited include:

- **Ambassador Ahmad Kamal**, Chair of the Working Group on Informatics, United Nations, for convening representatives of nations worldwide for two conferences at the United Nations to promote awareness and stimulate global Y2K cooperation.
- **Bruce McConnell**, Director, International Y2K Cooperation Center, for his leadership in promoting information and resource sharing and cooperation among national Y2K coordinators and industry sector leaders worldwide.
- **Senator Robert F. Bennett**, Chair, Senate Special Committee on the Year 2000 Technology Problem, for realizing early on that Y2K was not just a simple IT problem and for holding hearings and providing enough alarm to promote readiness without being directive.
- **Congressman Stephen Horn**, Chair of the House Subcommittee on Government Management, Information, and Technology, for his grading system of Federal agencies' Y2K programs, which also sounded an alarm, provided an effective public relations tool, and put pressure on agencies to make their mission critical systems Y2K compliant.
- **Bonnie R. Cohen**, Under Secretary for Management, and **John O'Keefe**, Special Representative for Y2K International Coordination, Department of State, who received plaudits for establishing the Interagency Y2K Working Group to foster Federal agency sharing, cooperation, and collaboration in helping ensure international Y2K readiness to the benefit of U.S. overseas operations.

- **Rear Admiral George Naccara**, Chief Information Officer of the U. S. Coast Guard, whose efforts to galvanize the International Maritime Transportation System into a cooperative partnership provided a cohesive force for Y2K readiness.
- **Rodrigo Moraga Guerrero**, President of the Council of Government Internal Auditors, Santiago, Chile, who was acclaimed for working in conjunction with the IY2KCC to share information and foster regional cooperation on Y2K in South America.
- **Late Prime Minister Keizo Obuchi of Japan**, for forging bilateral Y2K cooperation with the United States, making Y2K a national priority, and establishing an action plan and program management structure to stimulate Japanese business and government support for the Y2K readiness effort.

Thanks and appreciation were also extended to countless other industry and public servants worldwide who went beyond their normal duties and responsibilities to help manage the Y2K crisis. After many months of high-pressure and intense effort to meet the fixed deadline, all are to be commended for their contributions to the successful transition to the New Year.

Ensure Senior-Level Involvement

It wasn't left up to middle management to deal with; senior managers were actively involved. As a result, the issue gained substance.

— **A senior official**, Bureau of East Asian and Pacific Affairs, U.S. Department of State

Global, regional, or national leadership alone is not enough to successfully overcome a worldwide IT management challenge. The involvement and support of senior executives are also critical to ensure that technology-related initiatives are effectively implemented in individual organizations. Recognizing the seriousness of the Y2K situation, senior executives often worked directly with their project managers—obtaining technology advice, debating remediation options, and monitoring progress. Senior executives in some organizations had enough foresight to take direct interest in their organizations' Y2K readiness projects from the outset. A few went so far as to guarantee that operations would continue undisrupted at the rollover, or they would resign their positions.

Some organizations initiated Y2K programs without the necessary senior-level commitment, however. They learned the hard way that the best way to get action on big projects like Y2K is to get senior executives involved, providing direction to the rest of their organizations on what they needed to do. For example, according to Defense officials, the Department initially did not make much progress on Y2K readiness due to a lack of senior-level support. Only after the Secretary of Defense got involved in August 1998 and provided central direction for the Joint Chiefs of Staff to institute a joint project and ensure priority for Y2K management did the work get done. Within the Department of Transportation, the U.S. Coast Guard organized its technical approach much earlier, with the Commandant making Y2K management one of the organization's top three priorities in 1998. By 1999, the Coast Guard was well on its way, transitioning from a strictly technical approach to a risk management strategy that recognized possible Y2K impact on operational readiness in the maritime sector. Coast Guard officials

nonetheless stated that if they had geared up to address the problem earlier, it would have been a lot less stressful. Internationally, Mexican light and power officials indicated that only after demonstrating what would happen to the organization in the event of Y2K-related problems were they able to secure total senior-level support for ensuring Y2K compliance.

Provide Adequate Funding and Commitment

No one should regret the money or time spent on Y2K. If global systems are complacent about it, then they do not realize the potential consequences of the issue.

— **A financial management official**, Hong Kong

Y2K taught us that senior officials can best demonstrate their support for global management projects by devoting financial and human resources to their successful implementation. Although exact costs are indeterminable, it is generally agreed that significant resources—anywhere between $300 and $500 billion—were expended on the Y2K readiness effort worldwide. The United States alone spent an estimated $100 billion on Y2K management—about $8.5 billion of which can be attributed to the Federal Government. Some analysts also believe that other industrialized countries, such as the United Kingdom, Canada, Denmark, and the Netherlands, spent equivalent amounts per capita to the United States. The World Bank, through its Information for Development Program (*info*Dev), distributed more than $35 million in assistance from donor countries to over 100 developing nations through grants, technical assistance, and participation in regional and global Y2K conferences. Given the successful outcome of the worldwide project, officials worldwide concluded that the expenses were well worth it.

Problems arose, however, from the fact that individual countries and organizations handled Y2K funding differently. For example, although some countries had no separate fund, the U.S. Congress provided an emergency supplemental of $3.35 billion to support Federal agency Y2K management for the last 15 months before the deadline.[4] Department of State Information Resource Management officials stated that the emergency supplemental was crucial to the success of their Y2K program. According to the U.S. General Accounting Office, the Department of Treasury also cited funding as the major hurdle it faced throughout the Year 2000 challenge.[5] Without emergency funds and the ability to reallocate resources, Treasury would not have been successful in achieving Year 2000 compliance for some of its critical business processes and systems. Federal officials assert that providing emergency supplemental funds is a financial strategy that could be extended to ongoing programs to ensure critical infrastructure protection, as well as to address other crosscutting management challenges in the U.S. government arena.

Y2K funding was not always provided in a timely manner at locations worldwide. This was a problem for developing countries that were still anxiously awaiting Y2K assistance in September-October 1999, because the World Bank had not yet received all of the money needed from

---

[4] *Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999* (Pub.L. 105-277), enacted in October 1998.

[5] *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges*, U.S. General Accounting Office (GAO/AIMD-00-290, September 12, 2000).

donor nations to implement grants. Some needy countries did not get the funding requested to address Y2K management until December 1999. Y2K funding was also uneven across organizations. For example, private financial institutions—some of the first to begin remediation—spent billions of dollars on Y2K management. In contrast, other organizations such as U.S. diplomatic and consular posts worldwide often had to make-do with existing budgets or use year-end leftover funds to cover Y2K management activities. For future global IT management efforts, timely and adequate funding must be worked out in advance at all levels—global, national, and organizational—to keep frustrations over financial resources to a minimum.

The Y2K exercise also demonstrated that managers must recognize and be willing to accept up front the various nonfinancial commitments that global IT management may entail. One such commitment is the need to reassign scarce staff resources to accomplish the project. For example, although officials in the intelligence community recognized Y2K as a priority and set up a structure for providing resources to support the effort, Y2K managers still had to negotiate and form a virtual office to get all the help they needed from across their agency. Similarly, business units at a telecommunications organization in London complained that many key staff were diverted to Y2K activities, resulting in a visible lack of resources in all sections and a need to backfill positions. The U.S. Coast Guard extensively used its Reserve Program to provide specialists to meet key Y2K program needs. Further, without a permanent office structure or new personnel billets for Y2K activities, Defense Joint Staff officials said that they had to pull people together—often on a part-time basis--and "beg, borrow, and steal" for office space. One benefit for staff reassigned to Y2K management was the opportunity to develop new project management skills or undertake additional responsibilities that helped further their individual professional growth and development.

Managers nonetheless had to cope with the fact that while time, attention, and resources were devoted to Y2K, productivity was lost in many other areas. As officials in one telecommunications organization in London noted, maintaining commitment throughout a long-term project like Y2K crisis management was difficult. Some people who joined the project several years prior to the rollover lost interest due to "battle fatigue" and incessant routine reporting. The company ultimately had to develop a bonus scheme to retain valuable staff.

UNITED NATIONS

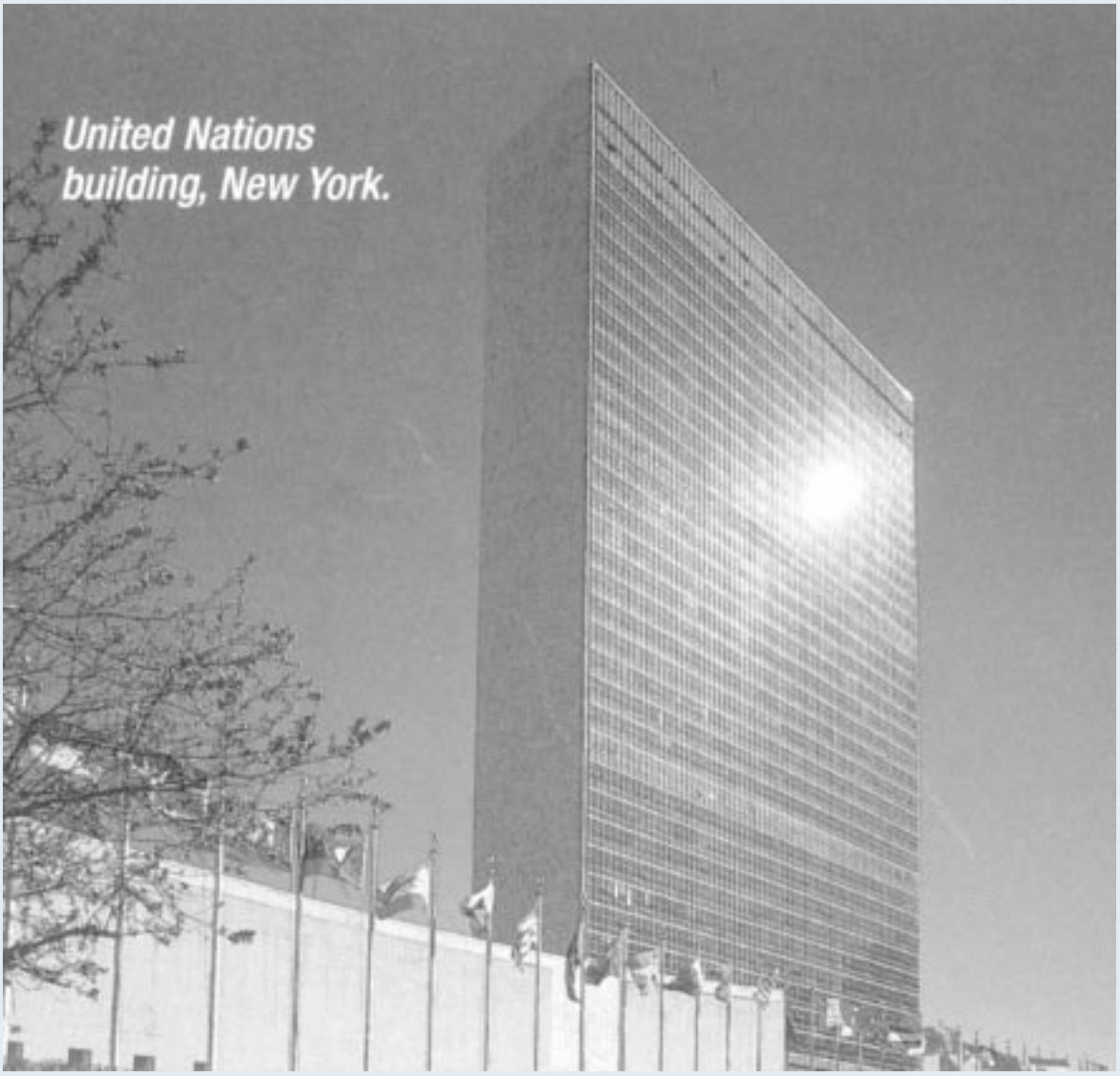


Figure 2: Photograph of the United Nations building, New York City

Source: State Magazine, February-March 2000

Case Study on UN Global Leadership

United Nations leadership in global Y2K management began through the efforts of the Working Group on Informatics and, in particular, its Chairman, Ambassador Ahmad Kamal. The Working Group was created under the auspices of the UN's Economic and Social Council to provide Internet access, training, and modern office systems to UN member states. With the modernization project accomplished free of cost through the use of surplus UN equipment and human resources, the Working Group shifted its focus to combating the Y2K threat.

Working Group members discussed options for addressing Y2K—not only at the UN, but in their individual countries worldwide—however, they lacked the funds with which to do much. Help came in the form of John Koskinen, Chair of the President's National Council on Year 2000 Conversion,[6] and about $220,000 in U.S. funding. After participating in the Working Group on Informatics as a guest and perceiving the need for international cooperation on Y2K management, Mr. Koskinen worked with Ambassador Kamal to organize the first global Y2K conference, held at the United Nations in December 1998.

To prepare for the meeting, Ambassador Kamal expanded an electronic mailing list developed for the Working Group on Informatics to include names of critical Y2K focal points in member nations worldwide. With the help of one staff member provided by the United States Mission to the United Nations, Ambassador Kamal and Mr. Koskinen organized the global conference in just 2-3 months—something that reportedly had never been done so quickly before at the United Nations. Keys to their success included use of e-mail alone to invite worldwide participants and financial incentives to get them to come. They also established a secure web page to post documents and reports and generate feedback from UN member nations on their Y2K status prior to the conference.

The first United Nations conference on Y2K had participation by 120 countries. The agenda included presentations by a chosen sector and open discussion on Y2K readiness. To encourage open dialogue among participants on their countries' Y2K readiness, there were to be no speeches or formal country statements. A key outcome of the conference was establishment of the IY2KCC.

The global conference at the United Nations was a Y2K "wake-up call" for many nations. It featured candid discussion, a good flow of ideas, and open disclosure on each country's Y2K readiness. Participants coordinated Y2K efforts at the regional and subregional levels and identified sectors such as maritime and health that had previously been ignored. They outlined milestones and activities for global Y2K management. They also agreed to follow up on Y2K progress through a second global conference in June 1999, funded principally by the United States, Britain, and Canada. This had participation by 170 countries—more than any other United Nations meeting on a single issue.

[6] At the time of his participation in the Working Group on Informatics, Mr. Koskinen had not yet been appointed at the National Y2K Advisor to the U.S. President.

Principle II: Appreciate the Value of Coordination, Cooperation, and Collaboration

Countries and organizations across the globe recognized that they stood to gain from sharing information on their Y2K readiness efforts. Even parties not accustomed to collaborating realized the importance of exchanging knowledge. They openly shared data, ranging from assessments of Y2K risks that they faced to strategies for resolving the associated problems. The unprecedented level of worldwide cooperation came with the realization by many that the Y2K technology problem also presented significant business and management risks. Public and private organizations formed worldwide networking partnerships to address the Y2K challenge. In addition, a few countries passed laws and implemented regulatory guidance to foster a climate that allowed organizations to share knowledge without legal hindrances or other concerns.

"It was an impressive mobilization of resources and people and a good demonstration of effective cooperation and communications."

— **A Foreign Service Officer**, U.S. Consulate Hong Kong

Promote Worldwide Cooperation at All Levels

Y2K was the first time that the international community all rose to the challenge and worked together to meet a common threat; international cooperative efforts did not compromise anyone's sovereignty or commercial interests.

— **Ambassador**, Permanent Mission of the Kingdom of Lesotho to the United Nations

The Y2K exercise was a good example of how people worked cooperatively on a major international problem and dealt with tight timeframes. Everyone had incentives to cooperate and share information. There were no real disincentives. For the United States, for example, it provided an opportunity for collaboration and information exchange across diverse Federal agencies and departments, among state and local organizations, through private sector industries and working groups, and within individual enterprises. Table 2 provides a summary idea of the extent of collaboration and cooperation at various levels worldwide.

Ensure Global Focus

Organizations such as the UN, IY2KCC, World Bank, and the International Monetary Fund were cited for their efforts in promoting global cooperation. As highlighted in the case study to Principle I above, the global conferences on Y2K held at the United Nations in December 1998 and June 1999, were better attended than perhaps any other meeting in the history of the organization. The infoDev Program, managed by the World Bank and funded by public and private donors, assisted governments around the world in addressing the Y2K challenge. National and regional awareness seminars were organized in developing countries and transition economies, as part of infoDev. Eligible national governments could apply to receive Y2K grants for planning or systems implementation activities. Department of State officials also pointed to the infoDev web site as a good link to information on Y2K readiness efforts worldwide. Further, toolkits were also developed on issues such as organizing Y2K programs and developing

contingency plans. These toolkits were available in various languages, thanks to funds from donor countries. International Monetary Fund officials were credited with generating goodwill and positive public relations by establishing a contingency financing facility to help countries that might experience Y2K balance of payments problems. Additionally, countries within regional groups (i.e., Africa, South America, and Eastern Europe) are now working jointly due to the efforts of international organizations such as the IY2KCC, the Bank of International Settlements, and the United Nations to bring them together. Table 2 provides a summary of these and other contributions of key organizations involved in Y2K management at the global level.

KEY GLOBAL ORGANIZATIONS	SIGNIFICANT CONTRIBUTIONS
United Nations	• Hosted global meetings of national Y2K coordinators • Established the International Y2K Cooperation Center • Utilized an electronic mailing list developed by the Chair of the UN's Working Group on Informatics
United Nations Development Program	• Funded regional Y2K efforts • Established a Y2K web site to coordinate UN country office activities • Provided grassroots support to local organizations
International Y2K Cooperation Center	• Managed global electronic communications to support Y2K national coordinators • Developed an information-sharing network across national boundaries
World Bank	• Provided financial support for UN global meetings • Supported Y2K efforts in developing countries through grants, loans, seminars, and technical assistance
International Monetary Fund	• Created a special loan facility extending short-term financing to countries facing potential balance of payments problems due to Y2K failures
Organization of American States	• Supported OIG and U.S. Information Agency efforts to host a series of interactive "Worldnet" discussions on Y2K issues via live uplinks at U.S. Information Agency facilities in Latin America and Canada

Table 2: Significant Contributions of Key Global Organizations

Source: *Y2K: Starting the Century Right!* Report of the International Y2K Cooperation Center, Washington, DC, February 2000.

Establish Mechanisms for Regional and Bilateral Collaboration

The IY2KCC formalized the structure for regional coordination on Y2K management based on discussions at the global meeting at the UN in December 1998. The Center identified eight world regions and established regional coordinators to promote awareness, cooperation, and information sharing on Y2K among the countries in their areas. A series of seminars and conferences were held in the different regions in this context. Levels of collaboration and cooperation varied from region to region due to language, cultural, or geographic barriers.

For example, Y2K officials at the United States Information Agency[7] told us about efforts by Caribbean countries to work together among themselves and with the United States to promote awareness and share information. Led by the Caribbean Development Bank, these activities were cited as successful endeavors, despite geographical dispersion, language differences, and variant levels of Y2K preparedness among countries in the region. Similarly, Embassy officials in Singapore discussed the first Asian Regional Y2K Coordinators Meeting, held in the Philippines in March 1999. The meeting had participation by 14 countries. The purpose of the meeting was to develop contacts, exchange country readiness information, and share effective Y2K strategies and practices. This meeting was followed up in April 1999 by a conference of Asian-Pacific Economic Cooperation nations, hosted in Singapore as part of the region's "Y2K Week." This conference focused on issues such as potential cross-border impacts of Y2K, problems unique to small and medium-sized enterprises, maintaining public confidence, contingency planning, and sector-specific challenges. The region's "100 Days Cooperation Initiative" promoted information sharing before and during the date change, using the IY2KCC as a resource. **Table 3** provides a summary of various organizations and activities related to Y2K management at the regional level.

There were also noteworthy instances of bilateral Y2K readiness coordination. For example, U.S./Japanese cooperation on Y2K issues began in Fall 1998 with joint statements by the President and the Prime Minister of Japan on bilateral cooperation in several key areas, including telecommunications, energy, transportation, finance, health care, and foreign assistance. In response, officials from a number of Federal departments and agencies, including the Department of Transportation, the Department of Energy, the Federal Aviation Administration, and the Centers for Disease Control, began collaborating and sharing Y2K management information with their Japanese counterparts. Officials from the two countries also exchanged visits to observe Y2K contingency planning and testing. U.S. management strategies and toolkits helped support Y2K assessments and remediation throughout the Asian-Pacific region. Concerned about the potential effects of Y2K on U.S. military base readiness in Japan, the Department of Defense (i.e., the Pacific Command), with support by the Department of State, also worked closely with Japanese defense agencies to assess military facilities and supply capabilities in the host nation. U.S. Department of Defense approaches to overseas Y2K readiness assessments are discussed in Principle IV below.

[7] The U.S. Information Agency is now the Office of Under Secretary for Public Diplomacy and Public Affairs within the Department of State.

REGION	BACKGROUND	SIGNIFICANT CONTRIBUTIONS
Asia	• 39 countries, of which 34 participated in regional activities • 4 regional meetings	• Under the Asian-Pacific Economic Cooperation Forum • Developed the *100 Days Cooperative Initiative* to promote information sharing • Held a September 1999 meeting with energy experts
Central America and the Caribbean	• 27 countries, of which 24 participated in regional activities • 10 regional meetings	• Developed a regional Y2K web page • Formed expert working groups with a focus on dependencies and cross-border services
Eastern Europe and Central Asia	• 28 countries, of which 26 participated in regional activities • 8 regional meetings	• Established a Regional Y2K Cooperation Center in Sofia, Bulgaria • Shared energy sector contingency plans and held joint training on their implementation • Held three Y2K conferences on the energy sector and nuclear power
Middle East and North Africa	• 19 countries, of which 12 participated in regional activities • 1 regional meeting	• Held a subregional workshop on natural gas production and distribution in Tunisia • Established sector leaders to build communications networks in energy, oil, water, and health
North America	• 3 countries, of which 3 participated in regional activities • 3 regional meetings	• Shared best practices and Y2K guidance • Provided leadership and funding to the World Bank and developing countries for international Y2K management
South America	• 10 countries, of which 10 participated in regional activities • 8 regional meetings	• Created a forum for communicating and coordinating national and sector Y2K activities • Formed technical working groups and held expert meetings in various sectors • Led public awareness and contingency planning efforts
Sub-Saharan Africa	• 48 countries, of which 38 participated in regional activities • 4 regional meetings	• Addressed dependency and cross border issues in a series of regional workshops • Shared contingency planning and information sharing strategies among Y2K experts • Shared Y2K resources and skills via workshops, web pages, and contingency planning seminars
Western Europe	• 23 countries, of which 19 participated in regional activities • 7 regional meetings	• Provided financial assistance via the World Bank and lent staff support for Y2K efforts outside of the region • Held regional workshops to address cross border dependency issues in electrical, gas, and nuclear power sectors
G8 Countries and G7 Finance Ministers	Canada, France, Germany, Italy, Japan, Russia (G8 member only), the United Kingdom, and the United States	• Shared national Y2K readiness information and assisted developing countries through the World Bank (G8 nations) • Shared statements on Y2K readiness at June 1999 economic summit (G7 nations)

Table 3: Significant Contributions of Key Regional Organizations and Structures

Source: *Y2K: Starting the Century Right!* Report of the International Y2K Cooperation Center, Washington, DC, February 2000.

Further, U.S. embassy officials in Mexico told us about host country initiatives to develop bilateral relationships with the United States as well as other Caribbean and Central American countries. Through coordination efforts and systems testing activities, aviation officials in the United States and Mexico established strong relationships and open lines of communications that are still active today. A series of bilateral meetings were also held among the U.S. Coast Guard, Canada, and Mexico, to share data, intelligence, and approaches to managing Y2K in the maritime sector. Additionally, at the December 1998 UN conference on Y2K, Mexico's National Institute of Statistics, Geography and Informatics, which was also the National Y2K Conversion Commission, took leadership of the Regional Y2K Forum supporting the IY2KCC. The Commission organized and delivered several Y2K conferences held in different countries in the region.

Chilean Y2K officials also established bilateral relationships with their neighbors in Argentina, Uruguay, Paraguay, and Brazil specifically to coordinate on Y2K management. These countries generally followed the Chilean model for managing Y2K in their own business/government environments but also cooperated with Chile in a number of common areas. For example, Chile and Argentina share several interconnected points for electricity along their borders. In a collaborative effort, energy officials worked to develop a registry of all energy lines (i.e., from gas producers to electrical power plants) between Argentina and Chile. The two governments also selected coordinators from among their respective sectors to jointly develop Y2K contingency plans in the energy area. Similarly, under Chilean leadership, South American countries worked together to coordinate border crossings in air transportation during the millennium transition—addressing such issues as permits to fly over neighboring air space and interconnections among air traffic control systems. Chilean officials observed that such Y2K collaboration has generally helped to improve relations among South American countries and that there is an interest in continuing the teamwork enhanced by the project in the past few years.

Promote Sector-Level Cooperation vs. Competition

Effectively addressing the Y2K issue required that organizations in different sectors cast competitive issues aside. The 10 sectors identified by the IY2KCC to facilitate Y2K coordination are listed in **Table 4**. Y2K sector representatives that we interviewed readily pointed to cooperative sector initiatives at the global level. For example, they told us about efforts by the Joint Year 2000 Council, under leadership of the Bank of International Settlements, to oversee and coordinate all aspects of the public sector approach to Y2K readiness in the financial management area. They also discussed how private financial organizations banded together under the Global 2000 Coordinating Group to jointly manage the Y2K problem. Of all sectors, the financial sector was the most vulnerable to Y2K due to its heavy reliance on digital computers; it was also the most prepared. The case study accompanying this principle area provides additional information on Global 2000.

Similar dialogues also occurred among banking officials at the regional level. For example, banking officials in Singapore, Hong Kong, and Chile shared their individual experiences in preparing for Y2K. The Monetary Authority of Singapore worked to develop national financial guidelines, which covered testing and contingency planning, and identified teams of regulators to document remediation progress in the banking industry. In addition, the Monetary Authority worked to educate multinational banks located within the country on local remediation efforts. **Table 4** provides a summary of contributions of key organizations and activities related to Y2K management at the sector level.

The Italian Y2K coordinator observed a phenomenon in which international institutions in sectors such as finance or air transportation that had more power and authority to carry out their role than others rose to the fore in helping the world prepare for Y2K. For example, central banks, originally created to control global speculative actions, took the lead in Y2K management versus global institutions in the telecommunications or rail transportation sectors that could not force industries under their purview to comply with their regulations. This official believed that Y2K was perhaps the first instance of ranking sectors in terms of their ability to react to a problem and concluded that these "stronger" sectors now have more responsibility for helping to keep the world in equilibrium.

SECTOR	KEY ORGANIZATIONS AND STRUCTURES	SIGNIFICANT CONTRIBUTIONS
Finance	• Bank for International Settlements	• Established a Joint Year 2000 Council to manage a public sector approach to Y2K • Arranged to accept additional forms of collateral as international liquidity demands required
	• Global 2000 Coordinating Group	• Created by private financial sector institutions • Promoted transparency and Y2K remediation via Y2K readiness charts
Energy	• No single global focal point • Key players included American Petroleum Institute, Organization of Petroleum Exporting Countries, International Energy Agency, and others	• Held energy-related conferences in IY2KCC regions and identified technical resources for national coordinators • Conducted worldwide information sharing on Y2K problems and solutions (American Petroleum Institute) • Established a 90-day oil supply to provide oil, as needed, on a global basis (Organization of Petroleum Exporting Countries)
Nuclear Power	• Key players included U.S. Department of Energy, International Atomic Energy Agency, Nuclear Regulatory Commission, and others	• Provided funding and/or technical assistance to the Y2K management efforts of nuclear power plants • Informed the public about Y2K preparedness of nuclear power plants (International Atomic Energy Agency)
Health	• British authorities, with World Bank support, led international Y2K efforts in this sector	• Provided support, via Web link, to national coordinators and developed a health sector contingency plan • Deployed "Health-check" missions to countries needing assistance in preparing for Y2K in the health sector
Telecom-munications	• International Telecommunications Union	• Conducted technical workshops in 14 countries • Set industry standards for compliance, testing, remediation, and contingency planning • Published survey results of countries' Y2K readiness on web site
Aviation	• International Civil Aviation Organization	• Assessed individual nations' Y2K progress, coordinated regionwide contingency planning, and assisted in contingency plan development
	• International Air Transport Association	• Provided seminars to foster collaboration and cooperation among airports, airlines, and civil aviation authorities
Maritime Shipping	• International Maritime Organization	• Identified responsibilities, promoted information exchange, and provided training through the Code of Good Practice • Provided Y2K contingency planning guide to identify problem equipment, failure scenarios, mitigating options, and contingency plans
Chemicals	• Intergovernmental Forum on Chemical Safety	• Issued chemical industry standards on Y2K
	• Organization of Economic Cooperation and Development	• Coordinated establishment of a clearinghouse on chemical emergencies
Customs	• World Customs Organization	• Organized a contingency planning workshop and produced guidance on Y2K compliance and business continuity planning
	• United Nations Conference on Trade and Development	• Initiated a technical awareness program and developed systems upgrades for widely used management systems
Government/ Public Services	• Vary from country to country	• Provided or managed national critical infrastructure services including power, telecommunications, health care, and defense • Shared information and best practices via regional conferences • Cooperated and coordinated to avoid cross-border incidents and instability during the rollover

Table 4: Significant Contributions of Key Sector Organizations and Structures

Source: *Y2K: Starting the Century Right!* Report of the International Y2K Cooperation Center, Washington, DC, February 2000.

Foster National Cooperation

In the United States, the International Interagency Y2K Working Group led by the Under Secretary for Management of the Department of State was characterized as an excellent forum for Federal information exchange. Collaboration through the Working Group enabled agencies to identify and use staff and resources from each other's agencies. For example, Defense teams identified expertise from other agencies to add to their contingents travelling abroad. Without the coordination and networking opportunities provided by the Working Group, this would not have been possible. The Working Group also helped focus government agency attention on why foreign Y2K problems were also U.S. problems. National task force members in Mexico and Italy identified sharing across departments and ministries within their countries as key to facilitating further sharing among local sector representatives. Italian electricity officials viewed the Y2K experience as positive because it also gave them the opportunity to establish points of contact and coordinate with other sectors and industries, such as rail transportation and telecommunications.

Take Advantage of Informal Networking

The Y2K exercise served to underscore the need for lines of communications beyond formal channels. A number of officials discussed the benefits of informal networking during the Y2K exercise. Interagency informal networking was a building block for accomplishing Y2K efforts throughout the U.S. Government and even across the globe. Frequently, it helped government officials understand the role, responsibilities, and scope of other agencies. Many officials identified business and personal contacts that will be useful to future endeavors. A U.S. industry official observed that sometimes the data collected was not as important as the contacts that were made during the crisis preparation period. This official contended that meeting the right people at the right levels, informal networking, and establishing lines of communications for future use were more beneficial than the information obtained through these channels.

For example, the Y2K experience will help officials in Hong Kong's Information Technology and Broadcasting Bureau better manage information security issues because it put them in contact with their counterparts in the United States and other countries, sectors, and trade organizations. Additionally, officials recognized that the Y2K project helped encourage relations among officials normally not in contact with each other. For example, banking officials in Mexico told us that their Quality Assurance Office, an internal management office that normally does not communicate with individual banks, was designated the Y2K coordinator for the country's entire financial sector. Designating the Quality Assurance Office as the Y2K coordinator resulted in improved sectorwide communications in preparation for Y2K and will facilitate management of other common issues.

Form Public/Private Partnerships

A key source of information was the private sector; good business partnerships were begun, and they need to continue.

— **Special Representative for Y2K International Coordination**, U.S. Department of State

The Y2K exercise brought about the formation of new public/private partnerships and improved paths of international and domestic communications. As time passed, there was an increasing amount of quality information available on issues such as leading practices for managing Y2K assessments, remediation and testing, as well as preparing and implementing contingency plans. This information saved valuable time, particularly for those that started Y2K management later than others, and reduced remediation costs.

Officials provided numerous examples of innovative and successful public/private partnerships around the world. For example, the U.S. Coast Guard partnered with the United Kingdom's Maritime and Coastguard Agency and large maritime trade organizations to develop a common approach to shipping safety and mobilization. Together with one of the groups, the Protection and Indemnities Clubs—maritime industry insurers based in the United Kingdom—they helped educate shippers on how to prepare for the rollover. They distributed Y2K toolkits at the UN conferences and worked with insurers to publish a booklet on contingency planning. Many key players in the shipping industry attended an international maritime industry meeting in London, while others developed independent measures to address Y2K. Ultimately, however, a common approach was taken, with maritime safety as the mutual goal. In another example, U.S. Embassy officials met with Singaporean officials and representatives of a Y2K Users' Alliance Team from large Fortune 500 companies, to discuss the status of their Y2K efforts. U.S. Agency for International Development officials in Egypt were also responsible for bringing together representatives from the Egyptian power sector with those of an international power company to discuss experiences and share lessons learned in addressing Y2K readiness.

But even while public entities played important and highly visible roles in global Y2K management, private industry—especially IT organizations—did much of the "heavy lifting" with respect to IT remediation. There was an enormous (and perhaps surprising) amount of coordination, cooperation, and collaboration among IT companies around the world. Some of this occurred in concert with government organizations. However, much of it occurred on an intra-industry basis. The role that many private companies played, both in helping to prepare systems for the Y2K transition and in providing guidance and helping to assess country readiness status, should not be overlooked.

Although business-to-business partnerships (e.g., companies and trade organizations) may occur on a regular basis, one Y2K expert told us that conferences and other dialogues to support Y2K readiness brought them even closer together. Trade associations—such as the American Chamber of Commerce and research institutes—were also instrumental in establishing Y2K standards and communicating results. For example, petroleum officials in Mexico worked with the Energy and Power Research Institute and the American Petroleum Institute to develop guidelines for rendering systems Y2K-compliant.

Ensure Legal and Regulatory Support

Legal actions regarding Y2K were almost unheard of outside of the United States.

— **A corporate executive**, Tokyo

Legislative measures related to Y2K were generally nonexistent in other countries. The United States, however, enacted a number of laws to address the potential for Y2K- related litigation and to promote an environment which encouraged sharing across borders and among companies. The Year 2000 Information and Readiness Disclosure Act, Pub. L. No. 105-271, 112 Stat. 2386, enacted in October 1998, for example, promoted disclosure and exchange of information on Y2K by limiting the liability of companies that publicized their Y2K status and readiness activities in good faith. Another piece of legislation, the Y2K Act, Pub. L. No. 106-37, 113 Stat. 185 (codified at 15 U.S.C. 6601 et seq.), passed into law in July 1999, was meant to discourage the filing of frivolous lawsuits and to encourage parties to resolve Y2K problems in lieu of litigation. A U.S. corporate executive, who worked to get the Y2K liability legislation enacted, stated that it greatly facilitated information sharing across border and company lines.

Industry leaders sought the support of the international regulatory community in preparing for the Y2K deadline—especially in highly regulated sectors such as finance. For example, banks in Chile worked with their Superintendent of Banks and Financial Institutions to reduce or modify regulations and thereby support their ability to modernize systems and processes to meet Y2K rollover requirements. Chilean banks hope that the collaboration and cooperation begun under Y2K among themselves and with regulatory organizations will continue into the future as they seek to make further technology investments to improve banking services and operations.

Additionally, Global 2000 officials said that regulators were effective in playing an educational role—promoting Y2K awareness, identifying effective management practices, encouraging remediation progress, and facilitating communications on activities such as contingency planning. These financial officials nonetheless believed that regulators could have coordinated better among themselves, done more to encourage Y2K readiness disclosure, and been more reasonable in their regulatory requests.

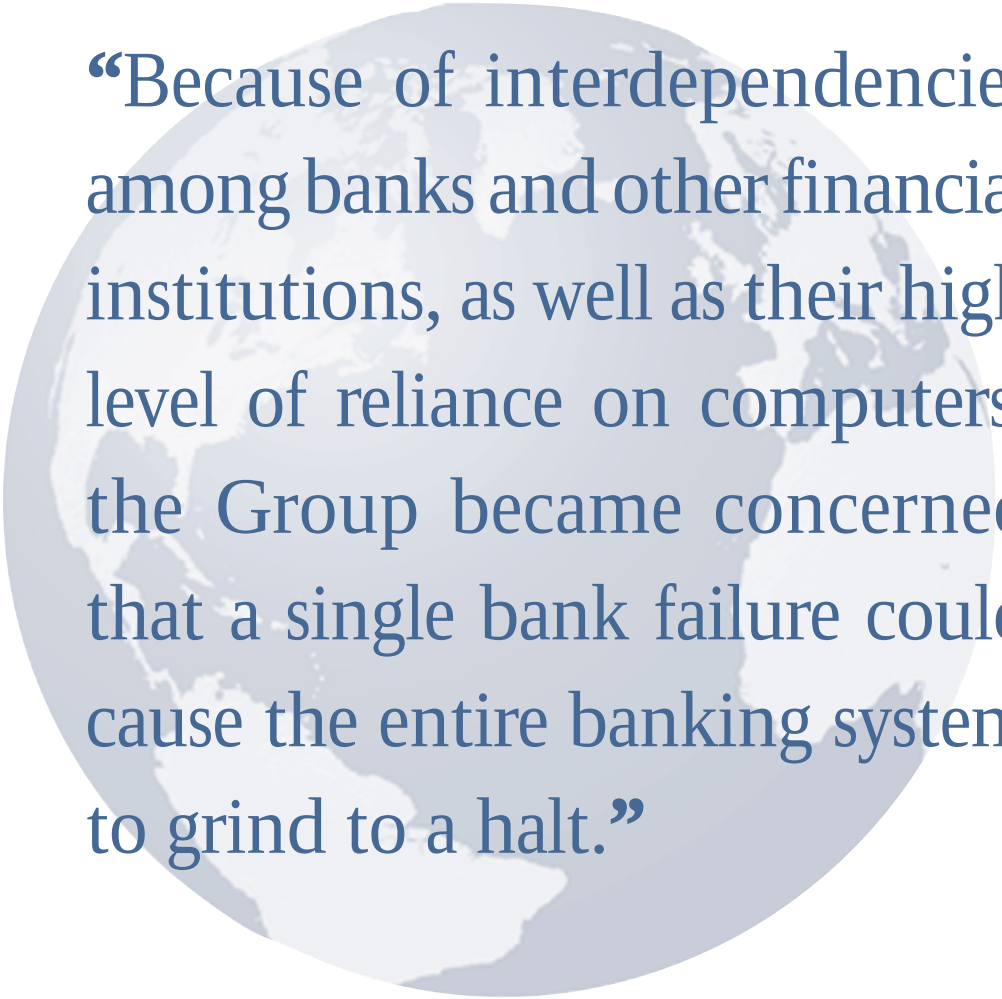
Further, International Telecommunications Union officials said that regulators sometimes posed obstacles to promoting Y2K awareness in their sector. For example, they said that countries in Eastern Europe and Asia tended to send too many regulators and government officials to International Telecommunications Union conferences, which were intended for telecommunications operators. As a result, International Telecommunications Union officials were delayed in their ability to get operators to attend the conferences. In some instances, Union officials visited the countries that did not send operators to the conferences to ensure that the operators in those locations were well informed.

Case Study on Global 2000

The Global 2000 Coordinating Group evolved from a series of discussions among firms and individuals that recognized the importance of raising public and private sector awareness and setting standards for addressing Y2K in the financial sector. Initially there were only pockets of Y2K activity within the financial sector; organizations were unaware of each other's efforts to address Y2K. Because of interdependencies among banks and other financial institutions, as well as their high level of reliance on computers, the Group became concerned that a single bank failure could cause the entire banking system to grind to a halt. Group leaders were also worried about potential impact on their efforts from other sectors (e.g., energy) and businesses. Through numerous discussions, financial sector leaders realized that the Y2K crisis was too daunting for them each to manage in isolation. They therefore agreed to set aside their usual competitiveness and work together in a cooperative spirit to achieve as much as possible before the deadline of December 31, 1999.

British financial executives spearheaded the Global 2000 effort in 1997 and provided funding throughout its first year. A senior British financial executive also served as Chair of the Group. Private and public sector participants were convened to join in the effort. Considered an ad hoc group of private banks, securities firms, and insurance companies, they also worked with regulators and international organizations. These included the Joint Year 2000 Council (representing the public side of finance on Y2K issues), various Central Banks and national groups, and the United Nation's Working Group on Informatics. The Group's mandate was to document leading practices in (1) developing Y2K assessments and disclosures, (2) conducting testing, (3) monitoring country readiness, and (4) performing contingency planning/events management. Ultimately, the group was successful because it shared ideas as widely as possible, having a strong commitment to inclusiveness, transparency, and disclosure.

In keeping with its commitment to disclosure, Global 2000 developed and circulated a Country Readiness Chart. This chart showed the readiness of 49 countries, based on their Y2K preparation activities in seven key areas—financial services, clearing and settlements, telecommunications, transportation, energy, water, and government services. The information in the chart was based on public information rather than private or confidential sources. The purpose of the chart was to promote dialogue and to stimulate the flow of information, which were critical for Group members and others to understand what was occurring in various countries worldwide. Many in the Group had different views about how the chart should be posted and who should have access to the data. For instance, some Group members believed the information should have been posted on the Internet, while others felt that releasing the information, particularly the ratings for developing countries, would cause capital flight. Ultimately, the chart was distributed to Group members and interested financial institutions, which were only allowed to share the information with customers and other relevant officials. The chart became an important instrument for getting organizations to take action to improve their Y2K ratings.



"Because of interdependencies among banks and other financial institutions, as well as their high level of reliance on computers, the Group became concerned that a single bank failure could cause the entire banking system to grind to a halt."

Principle III: Exploit Opportunities for Management Improvements

The Y2K readiness exercise helped institute a range of IT management improvements and effective practices from which organizations worldwide continue to benefit. Such improvements were not the explicit objectives of the exercise, but rather by-products of the focused and cooperative ways in which the world worked at various organizational levels to manage the IT challenge. These improvements touched upon the various aspects of information, technology, and project management, including such developments as increased awareness of the role of IT to mission accomplishment, improved information resources management, greater focus on contingency and emergency preparation, and more innovative use of technology to facilitate communications and sharing. These and other management enhancements remain possible as nations work together to address other global management issues.

"Even though [Y2K] turned into a nonevent with no major problems and relatively few minor glitches, for all intents and purposes, it yielded a side benefit in that we skipped a generation in terms of IT and innovative ways of doing business."

— **Special Representative for Y2K International Coordination**, U.S. Department of State

Recognize the Importance of IT to Business/Mission Accomplishment

Y2K raised IT awareness and, across the board, provided a more sympathetic view for the world of IT, technologists, and what they do for us.

— **Special Representative for Y2K International Coordination**, U.S. Department of State

One of the greatest benefits of the Y2K exercise was the visibility it provided for IT and the way it helped shape management views of the role of technology in their business endeavors. Prior to Y2K, many business managers did not understand the importance of IT and normally did not consider it in their everyday management deliberations. The Y2K crisis helped demonstrate how pervasive information technology is and that it is both a driver and enabler of government and business mission operations. Rooted in technology, Y2K threatened everything—from individual systems, to the electrical and communications infrastructures needed to support them, and to our individual personal lives. Managers were forced to appreciate the fact that if power grids failed due to Y2K-related disruptions, all work would stop, and mission operations everywhere could break down.

Perceiving Y2K as a business issue and not simply an IT problem, senior managers took steps to manage it as such. As indicated in Principle I above, senior executive involvement lent priority and visibility to Y2K readiness efforts. A number of organizations attributed much of their Y2K management success to the support that executive managers provided to readiness activities.

Senior executives often established steering committees comprised of managers from across business units to oversee Y2K budgets, activities, and progress to meet the fixed deadline. In cases of uncertainty, conflict, or emergency, executive involvement was useful to help make difficult decisions on Y2K project directions. IT investments, in general, came to be recognized as strategic, high-priority resources critical to business success or failure. Businesses such as a telecommunications organization in Hong Kong even used Y2K readiness as a means of increasing profits, for if the company was found to be more Y2K ready than its competitors, the company had an added advantage in the marketplace. The public relations department was said to be one of the company's most active departments during Y2K preparations.

Top-level involvement also helped ensure strong support for Y2K management across organizational units and departments. Operational and IT units that generally did not communicate with each other were forced to dialogue and build cooperation. IT managers learned to use common language instead of technical jargon for discussing with business managers the various systems issues related to Y2K. Through the interpersonal contact, business leaders learned about IT, and in turn, IT managers became more integral to business operations, no longer focusing strictly on systems issues. For example, an International Monetary Fund official told us that during Y2K preparations, their software developers worked with infrastructure and network managers more closely than ever before. IT managers met with officials in economics offices within the organization that they never would have encountered otherwise. The Y2K project also enabled the IT shop to demonstrate to senior managers that they were able to address a project this large and work with the rest of the organization to successfully pull it off.

Be Aware of the Risks Accompanying Technological Advancement

Use of IT implies risk; you cannot have a naïve perception of no risk if you use IT.

— **A National Y2K Commission official**, Mexico City

The Y2K crisis revealed that although there are significant rewards to using IT, there are disadvantages as well. For instance, the Y2K experience increased awareness of the extent to which systems are integrated, interdependent, and interoperable, raising concerns that systems failures in one organization could, in domino fashion, corrupt or cause failures in systems in another organization. Because one organization's Y2K success was everyone's success, a horizontal approach was necessary for Y2K management. For example, Hong Kong Monetary Authority officials said that during Y2K, they identified a series of events where banking disruptions could have impact on securities and futures markets. They realized that they had to collaborate on what to do if systems were to fail. As some officials suggested, ensuring continuity of interrelated systems and processes in the event of widespread Y2K disruptions could have been a nightmare.

Y2K also helped managers better understand IT supply chain and contractor dependencies and the vulnerabilities they imposed. For perhaps the first time, organizations had to think about checking with second or third tier vendors to get assurances regarding the goods and services that they provided. They found that although some vendors were forthcoming in the Y2K readiness effort—sharing Y2K status information about their products through conferences and reports or working with customers to upgrade their systems—others were less supportive. Organizations requested guarantees or assurances that vendor products were Y2K compliant, but sometimes could not get them. They relied on vendors to supply or to help implement Y2K fixes, but frequently experienced delays in service. For example, Y2K task force officials in Singapore stated that some health care equipment manufacturers—especially the small, little known ones—were as late as the third quarter of 1999 in fixing systems. Similarly, officials in one manufacturing industry in Tokyo stated that a technology supplier released a Y2K software update on December 27, 1999, which did not allow them enough time to install the update or ensure that it would work without problems through the rollover. Organizations also needed vendors to be on hand to help with problems in the event of Y2K-related disruptions but were dismayed at the lack of available technology repair capabilities. Through these experiences, organizations came to better appreciate the levels of their supplier/contractor dependencies and the need for improved oversight and control of the relationships. Such enlightenment is especially beneficial in the current era of just-in-time inventory where people no longer have the luxury of simply withdrawing supplies from warehouses when they need them.

Further, the Y2K crisis helped emphasize the vulnerabilities and issues that come along with greater use of technology. The Y2K crisis itself was a manifestation of the risks and vulnerabilities inherent in extensive use of technology. It highlighted additional concerns such as the embedded chip issue, which, fortunately in the case of Y2K readiness, did not turn out to be a big problem. It disclosed interrelationships among different types of risks. For example, U.S. Federal Reserve System officials stated that due to Y2K, senior executives and boards of directors of financial institutions now have a better understanding of the linkage between operational risks and other credit, market, liquidity, reputational, and legal risks. Y2K also focused attention on computer security and other emerging IT issues and the need for global strategies to address them.

Take Advantage of Opportunities to Examine and Improve Business Processes

Sometimes people work in the traditional way and do not look forward. Under Y2K they had to think and question processes. At times, people were even surprised that they could do things differently.

— **A financial management official**, Mexico City

Officials worldwide said that Y2K management gave them the unique opportunity to examine national infrastructures, industry sectors, and business and government operations. They learned as they went, obtaining broader perspectives on information technology use and enterprisewide views of their organizations, sometimes for the first time. They also made invaluable points of contact with external organizations for addressing other issues, as discussed in Principle II. The

knowledge that officials gained of their business environments was useful, not only for clarifying or documenting existing processes, but for identifying areas for general management improvement. For example, as a result of Y2K, U.S. embassies were able to identify and fill needs for critical supplies, equipment upgrades, or security enhancements. Similarly, Egyptian health officials identified potential electrical problems (lack of back-up power generation) in 115 out of the country's 220 hospitals. Using Y2K funds, they were able to bring in new generators and replace some older equipment and supplies, such as infusion pumps for dialysis.

Some organizations were able to reengineer their business processes as a result of the Y2K crisis. For example, as a result of Y2K-related systems replacements, the Organization of American States made improvements in its financial management processes, shifting from 28-year old custom-made management information systems to commercial off-the-shelf products. End-users also learned to use Windows technology for the first time. Further, Y2K readiness was the incentive for a Mexican financial institution to progress from the outdated mainframe technology they relied on for 35 years to more distributed processing.

Additionally, the Y2K exercise stimulated creative thinking about new business solutions and ways to advance through the use of technology. For example, Chilean banking visionaries used Y2K readiness as a platform for modernizing systems, expanding services, renovating old laws and regulations, welcoming new business and investments, and transforming their country into a major international financial center. Similarly, Mexican banks developed the idea for a central organization to monitor and share information in the banking sector. According to a diplomatic official from Pakistan, establishment of a national IT focal point under Y2K management led his country to begin debating other IT issues, such as cutting taxes on web access costs as a means of increasing Internet use.

Improve Systems Management

In effect, we should not call what happened a Y2K success, but rather a management success.

— **A Consular Affairs official**, U.S. Department of State

One of the foremost steps recommended in Y2K readiness was for organizations to identify and ensure compliance of their mission critical systems. This required managers to establish priorities, focusing only on those operations that are absolutely mission-essential and would therefore have to be sustained in the event of a crisis or emergency. It also required managers to look beyond the needs of decentralized business units to a broader, more holistic view of their organizations' operations. Some highly decentralized organizations such as the Department of State and, according to a U.S. General Accounting Office report, the Department of Defense had difficulty pinpointing critical crosscutting systems and processes.[8] They encountered obstacles to moving beyond turf battles and organizational "stovepipes" and focusing more narrowly on the critical needs of their agencies as a whole. Where successfully accomplished, knowledge of critical systems can help focus enterprisewide thinking and facilitate management of IT issues in the future.

---

[8] *Defense Computers: Year 2000 Computer Problems Threaten DD Operations*, U.S. General Accounting Office (GAO/AIMD-98-72, April 30, 1998

In the course of identifying mission critical systems, many organizations developed complete, up-to-date inventories of their IT resources, sometimes for the first time ever. With the inventories accomplished, organizations took the opportunity to streamline their systems portfolios, eliminating redundant, inefficient, and useless equipment—something that many had long wanted to do. For example, information management officials in the U.S. Embassy in Mexico said that the post got rid of 40 to 50 of their older computers under Y2K management. Further, the national Y2K coordinator in Italy said that large Italian companies were able to dispose of about a third of their software and make significant revisions to their systems portfolios as a result of Y2K. Organizations generally ended up with more knowledge about the types and categories of their hardware, software, and embedded systems, sometimes along with product information on suppliers and manufacturers. Organizations also gained visibility of networks and architectures and were better able to exercise configuration control. Many organizations have established databases of the systems information compiled under Y2K and plan to keep the information current for future reference.

Having inventories in place made it easier for organizations to assess and get their systems ready for the Y2K deadline. They found that many systems—especially those using older technology—were not date-sensitive and required no fixes at all. Where fixes were required, in many instances, organizations simply replaced the systems instead and trained their employees on the use of the newer equipment that could accommodate the millennium date change. As such, Y2K management served to kick off a wave of systems upgrades. Modernizations that had already been planned were sometimes expedited to meet the Y2K deadline. For example, the Y2K crisis led the Department of State to speed up its program for migrating embassies and consulates from proprietary legacy systems to more modern, secure, open systems technology for unclassified operations. In some cases worldwide, systems upgrades were not truly necessary for Y2K purposes; whether they needed it or not, many organizations got the next generation of computer equipment.

Overall, the IT modernizations resulted in more robust, efficient, and commercially available equipment. For example, an investment banking organization in the United Kingdom spent about 650 million pounds to replace 90-95 percent of their systems under Y2K. Every server and desktop computer in the company is new and is expected to have large pay back. Further, officials of an air traffic control organization in Mexico believed that the $15 million that they spent on Y2K management was also a good investment. The organization now has faster and better systems for radar signaling, information processing, and flight planning. Altogether, the organization completed a total of 400 computer replacements and upgrades without contracting out for services. The technical capabilities of the organization's technicians are also better because they sent the technicians responsible for the in-house systems fixes to training in France and England where the equipment was manufactured. In general, officials indicated that now that they have more up-to-date equipment, they plan to keep it refreshed so that they will not have to undertake such major modernization projects all at one time ever again.

Emphasize Systems Testing and Verification

The efforts to plan and do simulation testing provided a lot of visibility over potential problems and an opportunity to address them in advance of the crisis period.

— **Former Chair**, Working Group on Informatics, United Nations

Subsequent to systems remediation or upgrades, organizations placed a great deal of emphasis on testing and verifying systems performance to meet rollover requirements. Test procedures now exist in places that never had them before. Some organizations tested their systems beforehand to simulate Y2K problems and identify areas for remediation. Cautious not to just take the vendors' word or assume the adequacy of in-house fixes, organizations also conducted extensive simulation tests after remediation to ensure that systems would continue to operate through the rollover. For example, a financial institution in the United Kingdom spent $1 million to develop a Y2K test laboratory. As a result, the company now has a good structure in place for testing future IT projects, such as the monetary conversion by countries within the European Union to the euro.

Testing was not limited to individual organizations or vendors, however. Due to sector interdependencies, there was also considerable interagency and international testing. For example, officials of a Mexican telecommunications organization said that they participated in parallel simulation testing with other members of the International Telecommunications Forum. Member companies simulated their individual networks and established telecommunications links with other carriers in locations across the globe. It was a huge effort, requiring about 6 months to prepare and 6 days to perform, and involving 2,000 calls and various combinations of communications to test all critical rollover dates. Though the test was a complete success, the telecommunications company was not completely satisfied and therefore conducted its own 24-hour live test between two cities in Mexico. The company rolled the clock forward to move an entire city of 60,000 subscribers to the Y2K rollover period. The test, conducted without subscriber awareness, was also successful, demonstrating Y2K compliance in all systems, from supervisory oversight to billing. There were no customer calls or complaints to the telecommunications company during the test period.

Many organizations added another dimension to their Y2K testing by making greater use of independent verification and validation. Whether performed by internal units or external contractor organizations, independent verification and validation provided companies with some assurance that their Y2K remediation efforts were adequate. For example, through independent verification and validation processes, the U.S. Coast Guard identified Y2K problems that its own centers of excellence had missed. Further, through a certification process established at the Department of State, OIG worked with the Y2K project management office to identify and ensure resolution of 600 deficiencies in bureaus' systems certification packages. OIG also helped ensure that all of the Department's mission critical systems underwent the necessary steps to be made compliant prior to the millennium deadline.

Enhance IT Project Management Practices

[Y2K] was not easy, but it was a good experience that can be applied to managing other IT projects.

— **A telecommunications official**, Hong Kong

The Y2K crisis provided organizations worldwide with broader project management experience and the opportunity to reemphasize good project management principles that have been in existence for years. Seldom had managers had experience in dealing with a project of this magnitude, involving not just entire organizations, but nations and organizations across the globe. Given potential Y2K implications, it was critical to manage the project successfully the first time. As such, central project management offices were established to coordinate and communicate the effort at all levels. Project management skills needed for Y2K teambuilding were upgraded. Concepts such as performance measurement and modularization were applied to keep systems remediations on schedule and within budget.

Other project management principles were reinforced as well. According to a banking official in Mexico, the nonsystematic way in which many IT suppliers and programmers encoded dates in the systems that they developed was responsible for creating the Y2K problem. Some managers consequently began applying standard approaches to software engineering, programming, testing, and interpretation of results as part of Y2K management and plan to continue such standardization for other IT projects in the future. Standardization was applied to broader project management practices as well. For example, serving as its corporate focal point for Y2K, a telecommunications company in the United Kingdom instituted a common strategy, reporting methodology, and audit approach for Y2K management, leaving flexibility for other locations to tailor it to their local programs. The company's framework for managing Y2K across corporate groups is now documented, with plans to transfer the lessons learned to carrying out other projects. Further, the new manager of the Department of State's project for modernizing field office IT came on board just as the project office was deploying equipment to the first few posts. Recognizing that the project's goal for a consistent platform and standards required standardized and centralized implementation also, the project manager revamped the project plan based on a commonly accepted methodology in the Department.

Documentation was also reemphasized as an important management practice during Y2K readiness. Careful to leave paper trails during Y2K management for fear of audits and legal liabilities, a number of organizations now have standard requirements for documenting other IT projects as well. For example, there is now a desk in the Information Systems Department of Mexico's central power and light company with responsibility for quality control of systems applications in production. It is now standard procedure to update systems information in technical and users manuals. Though such documentation may take time, it is essential for current and future managers to understand how IT functions in their organizations.

Recognize the Importance of Contingency Planning and Emergency Preparedness

[Y2K] created a mindset of questioning and walking through various "what if" scenarios.
— **Special Representative for Y2K International Coordination**, U.S. Department of State

During Y2K preparations, countries and organizations worldwide placed greater importance on the need to safeguard systems, personnel, and infrastructures and ensure continuity of operations in case of widespread emergencies, disasters, or disruptions. This focus on emergency preparedness intensified during the second half of 1999, as anxieties about the rollover increased and places that had not previously considered contingency planning began to do so. Organizations engaged in a range of emergency planning activities. They conducted business continuity planning—securing infrastructures, implementing backup systems and processes, and instituting disaster recovery mechanisms to guard against operational disruptions. The continuity planning often included stopgap measures, workarounds, or manual recourses to help avert or minimize potential disruptions. Organizations also developed crisis management plans, ensuring the availability of supplies, backup communications, civil defense services, and evacuation strategies to manage or sustain communities in emergency situations. Crisis management activities often included development of different scenarios and test drills to determine the effectiveness of emergency management procedures when put into practice. Because emergency planning introduced many new concepts and strategies, it often entailed training for employees and managers in locations worldwide. The United States helped in this regard, providing guidance and instruction through overseas missions and conferences, and automated "toolkits."

By way of illustration, representatives from the G8 nations held a maritime contingency planning workshop during a Y2K working group meeting in Berlin, Germany in September 1999. The purpose of the workshop was for G8 participants to develop and adopt a common strategy for Y2K contingency management in the maritime sector. The U.S. Coast Guard took the lead in the workshop, showcasing its results and lessons learned from joint, public/private Y2K contingency management exercises at ports in San Francisco, New York, and New Orleans as a means of demonstrating the importance of Y2K contingency planning. Coast Guard officials also proposed that each G8 country sponsor its own maritime contingency management exercises and provided information packages to support their efforts. The packages included templates for conducting port-level contingency planning, contingency management exercises, information collection and dissemination, and public awareness, as well as helpful points of contact and a suggested timeline for making port-level preparations for the Y2K transition.

A number of locations instituted emergency management plans for the first time during Y2K readiness preparations. For example, although Egypt had no strategies in place for dealing with the various emergency situations (earthquakes, train accidents, plane crashes, and floods) that

they experienced in the past few years, the country began to mobilize and develop crisis management plans under Y2K. Other places, such as an Italian energy organization, updated or reinforced existing emergency plans and procedures. The organization upgraded emergency procedures put in place after a major oil incident 10 years ago. The updates were to accommodate any Y2K-related business disruptions, which could potentially be compounded by loss of communications, blackouts, etc. Emergency plans were instituted at many different organizational levels and ranged from simple emergency checklists to more sophisticated procedures. For example, Asian-Pacific countries worked together on comprehensive strategies for ensuring continuity of operations in the event of Y2K-related disruptions in regional civil aviation. The countries did not have such plans in place in 1997 when an air traffic control strike in India stopped air transportation in the region for 3 days.

Although many emergency plans were developed specifically for Y2K, locations worldwide are now in a better position to address the range of disasters or disruptions that could occur in the future. Recognizing that emergency preparedness is not a one-time effort, business continuity and crisis management planning is now a continuing requirement in a number of organizations. For example, civic protection plans that an Italian telecommunications organization established for Y2K are now part of an ongoing safety/protection structure. Further, Egypt held its first National Crisis Management conference in mid-July 2000 and planned to propose development of crisis management units in each Cabinet Ministry, except for the armed forces which already had such a unit.

Make Innovative Use of IT Tools and Techniques

South America used technology as it had never done so before. Teleconferencing became a daily tool. The Internet changed the ability to work together and share information.

— **Regional Coordinator for South America and President of the Council of Government Internal Auditors**, Santiago, Chile

The global Y2K management project served as a change agent, encouraging greater reliance and more innovative use of IT tools and strategies than ever before. Video and teleconferencing equipment were key tools in facilitating Y2K management communications and cooperation. For example, banking officials in London used regularly scheduled conference calls to coordinate Y2K management activities with up to 50-60 representatives of the corporation in locations worldwide. Follow-up was important and during the last month before the rollover, banking representatives were making daily calls to each other to share updated information on their Y2K progress. Chilean organizations also extensively used videoconferencing to share information and coordinate Y2K management regionally with their counterparts in Brazil and Argentina. Teleconferencing became a daily tool for these South American nations, as well.

Further, in accordance with a Memorandum of Understanding signed in April 1998 by the Secretary of State and the Minister of Foreign Relations of the Republic of Chile, and in agreement with the Organization of American States, OIG and the former U.S. Information Agency hosted

a series of interactive "Worldnet" discussions on Y2K issues. From November 1998 to March 1999, five programs were broadcast to address Y2K contingency planning, readiness in the energy and financial sectors, and the challenges of Y2K auditing and certification. Each Worldnet program featured field experts in the studio in Washington, DC, and audiences from three countries that actively participated in the discussions via live uplinks at U.S. Information Agency facilities throughout Latin America and Canada.

As some officials put it, we entered an era of "e-diplomacy," using e-mail to make arrangements and invite participants from around the world to conferences such as the two global meetings at the United Nations on Y2K. Officials worldwide also coordinated with each other, using e-mail extensively to share information in lieu of holding face-to-face meetings. There was a high degree of transparency—information was exchanged and ideas flowed at "e-speed." Officials that we interviewed believed that much of what was accomplished under Y2K management would not have been possible if we had continued to rely on more formal channels such as letters or the lengthy diplomatic cabling and clearance process. They indicated that the main problem with e-mail, however, is that it is informal and is therefore easily lost, leaving no paper trails.

Officials also suggested that it would have been difficult for the world to get through Y2K management without the Internet. As one Department of State representative indicated, one of the foremost messages from the Y2K experience is that we are all linked and there are gateways into every country via the web. Similar to e-mail, the Internet changed our ability to work together and share information consistently and simultaneously across the globe. Organizations developed Y2K web pages and updated them continually. People who had been timid about using computers were drawn into this means of communications, receiving training and using online technology for the first time.

As an official at the British High Commission in Hong Kong indicated, "web use went crazy" and was used to support Y2K management in a number of ways. For example, the web facilitated U.S. Coast Guard research to identify a critical Global Positioning System receiver that had a Y2K problem. It supported partnering arrangements for organizations like an Italian telecommunications company, which used an internal web-based project to exchange information between its IT shop and the network. UN officials used the web to disseminate documentation and reports in preparation for the two global conferences on Y2K. Further, as discussed in more detail in Principle IV below, Y2K assessments and status reports on countries around the world were also posted to the web. Such postings helped promote Y2K awareness and often put pressure on international entities to intensify their efforts to prepare for the Y2K transition. They also started an international "grass roots" movement to more openly disclose information. For example, Chile's national energy center used a secure web page to collect and update information on the Y2K status of the country's oil and fuel companies, creating links to other sectors' web sites so that they, too, could get access to this information. The British High Commission in Hong Kong experienced an extraordinary number of hits to its web site after posting the Y2K assessments sent in from its field offices. According to officials in the High

Commission, the postings worked well, raising the profile of the High Commission's front office in the United Kingdom.

Countries and sectors that had started remediation early often used the web to transfer Y2K guidance, tools, and software patches to countries that had made less progress in addressing the problem. The technology transfers, often translated into different languages and distributed free of charge, facilitated the ability of many nations to "leap-frog" ahead in Y2K progress—especially in the last few months of 1999. For example, the Department of Commerce, with funding by the National Institute for Standards and Technology, developed a compact disk to help managers determine their level of exposure to Y2K risk. Approximately 200,000 compact disks were distributed domestically; another 100,000 were used at more than 40 outreach conferences held in nearly 30 countries. Similarly, recognizing that many of its country offices had limited awareness of Y2K risks, UN Development Program officials shipped to the offices exactly what they needed to deal with the problem. UN Development Program officials followed up with workshops in five world regions to give staff a better understanding of Y2K issues. Further, Egyptian health officials said that videos of conferences with British and U.S. Agency for International Development experts were filmed and disseminated to others to provide greater information and understanding of Y2K in the sector. The videos were not just lectures. They also included equipment identification, pictures, and discussions, which proved to be highly effective training methods.

Figure 3: Management Improvements Resulting from Y2K Efforts

Source: Office of Inspector General

Case Study on a Mexican Power Company

A power company, providing about 27 percent of the electricity used in Mexico City and the surrounding area, had an early start in Y2K management. The Y2K committee, established in 1997, got senior leadership support by demonstrating potential impacts of Y2K-related power failures. With senior-level oversight and coordination among business units, Y2K management became an organization-wide priority.

The Y2K committee found a lot of information on the Internet to help with their Y2K management approach. Because the company's telecommunications infrastructure was so old, it required no remediation. On the information systems side, however, they had to purchase a new mainframe to become Y2K-compliant. By mid-1997, they also upgraded to top-line servers and computers, and migrated software from their old architecture. Their main IT suppliers cooperated greatly in these efforts. Employees were also trained to use the new equipment and to fulfill new responsibilities resulting from the upgrades.

In December 1998, the power company conducted joint testing and received certification from another utility that provides electricity to the rest of the nation. Still not satisfied, the power company performed additional tests with several U.S. companies, had the National Institute for Electric Research conduct an independent evaluation, and, along with the other electricity company, had a major IT supplier perform a three month-long audit of its conversion programs. All assessments checked out fine. The company already had contingency plans to sustain electrical power generation in case of trade union strikes. They instituted and tested upgraded plans for Y2K purposes.

Many people were on duty to support the rollover. Forty telephone operators were assigned to deal with public panic and inquiries. Another forty employees helped ensure the safety of approximately 2 million people gathered downtown to ring in the New Year. Army guards were called in to protect the company's physical installations. And about 350 people monitored information systems, using a web-based application to report rollover outcomes. Though no major problems resulted, two minor glitches—incorrect dates on two quarterly reports—were discovered in March 2000 and corrected in 2 weeks.

The power company has reaped many side benefits from its successful Y2K program. The Information Systems Department is now completely documented. Coordination between the Information Systems and Telecommunications Departments is more prevalent; both must now sign off on agreements for any new services or equipment. Quality control assessments and updates in technical and users manuals are standard requirements for new applications. Through a joint IT infrastructure, Mexico's two electric companies now have access to each others' networks and can jointly service all customers. E-mail, Intranet, and web use have helped enhance internal and external communications. The power company has also prepared a "white book" on all resource investments and outcomes from the Y2K project in anticipation of follow-up audits.

"Still not satisfied, the power company performed additional tests with several U.S. companies, had the National Institute for Electric Research conduct an independent evaluation, and, along with the other electricity company, had a major IT supplier perform a three month-long audit of its conversion programs."

Principle IV: Coordinate Guidance, Monitoring, and Data Reporting and Analysis Activities

Global Y2K crisis management was an incremental learning process. Through retrospective study of the project, additional areas for management improvement can also be clearly identified. For example, guidance to field operations and global status monitoring and reporting are areas in which the United States Government, and the Department of State in particular, may need to make adjustments to approaches devised to address other emerging global issues.

"There was a lot of interest in the Y2K effort from headquarters, which generated numerous inquiries, but the effort appeared uncoordinated."

—**A Foreign Service Officer**, U.S. Embassy Tokyo

During its preparations for the Y2K transition, the Department's headquarters undertook a concerted effort to support, guide, and assess the readiness of U.S. diplomatic missions and host nations worldwide. However, overseas officials that we interviewed consistently indicated that, for future efforts, the Department should take steps to better ensure that management guidance to its embassies and consulates abroad is reasonable and applicable to different host country environments. Federal organizations can also work together to eliminate redundant reporting requirements, consolidate international data gathering activities, and better analyze and synthesize the information compiled. Use of central command centers for crisis monitoring is one practice at which the whole world excelled and which needs to be continued in future endeavors.

Effectively Support Decentralized Crisis Management Activities

The Department faced several unique challenges in its efforts to prepare for the Year 2000, such as bureau coordination, systems inventories, worldwide deployments, contingency planning for all business processes and overseas locations, and monitoring rollover activities.

— **Y2K Program Management Office officials**, U.S. Department of State

In the context of the integrated global systems environment, managing the Y2K problem was a major undertaking for individual organizations, regardless of their size or structure. Supporting concerted, agencywide Y2K crisis management activities was especially challenging for highly decentralized international organizations like the Department of State. This is likely to hold true for addressing any future global issues, too.

Specifically, the Department of State relies heavily on its own internal IT systems as well as host country infrastructures to sustain mission critical operations and support American citizens at diplomatic and consular locations in over 160 countries worldwide. Therefore, assessing the Y2K readiness of embassy, consulate, and host country systems and preparing for Y2K-related failures through the Y2K transition were top priorities. Under the leadership of the Under Secretary for Management and the Chief Information Officer, and with participation by other U.S. agencies, the Department of State undertook a major effort to review the Y2K readiness of every overseas post and host country. Assessment teams were either created at, or provided to,

every U.S. diplomatic mission worldwide with the objectives of identifying Y2K vulnerabilities, monitoring remediation progress, and, as needed, assisting host country efforts to manage the critical Y2K transition. Of primary concern to the Department were continuing host country infrastructure operations in sectors such as energy, water, telecommunications, and transportation.

The Y2K Project Management Office provided a centralized body to give technical support and guidance, manage the schedule, and track and report progress on Y2K management efforts. The Department's Y2K readiness effort included expert assistance in identifying and remediating internal systems, centralized web sites with technical information, best practices, etc. The Y2K Program Management Office oversaw the testing of every corporate application and witnessed firsthand the problems encountered. The Office took similar measures to assess and ensure the operational preparedness of overseas posts for the Y2K transition. A first step involved development of a contingency planning toolkit. The toolkit provided a structure for posts to assess the status of systems and infrastructures, identify potential points of failure, and determine contingency resource requirements, such as food, water, cash, fuel, power, and communications, in case of Y2K-related host country infrastructure failures. The U.S. Congress provided Y2K emergency supplemental funding for procurement of resources to continue operations should such failures occur. Additionally, decisions on authorized departures of staff, and responses from oversight organizations were to be formulated based on toolkit information. In general, overseas Y2K contingency planning helped highlight additional opportunities to apply management solutions for long-term improvements to embassy and consulate operations.

Improve Guidance for Field Operations

Washington forgot that there were people on the ground who could best determine what to do.

— **A Foreign Service Officer**, U.S. Embassy Mexico City

U.S. embassy and consulate officials discussed with us the guidance they received from Department of State headquarters on how to prepare for the millennium rollover and sustain their operations through potential Y2K-related emergency situations. Some U.S. embassy and consulate officials appreciated the headquarters' direction, finding the guidance on contingency and emergency action planning quite useful. However, not recognizing that the volume and intensity of the guidance was often due to the learning curves and uncertainties that the Department of State, like the rest of the world, faced in the months preceding the Y2K deadline, other embassy officials expressed frustration with how the guidance was managed. Consistently, at every overseas location that we visited, they stated that the guidance seemed overly reactive and unreasonable. They offered various suggestions on how it could have been improved. For example, they said that the guidance could have been accompanied by the materiels, funds, and technical assistance needed to implement it.

By way of illustration, IT officials at one U.S. embassy said that they spent over 100 hours remediating dozens of unclassified computers—efforts that could have been greatly reduced if headquarters had supplied training or a server-based software distribution system to accomplish the fixes. Embassy officials said that some requirements, such as testing fax machines, copiers, elevators, telephones, and automobiles for Y2K compliance, seemed unreasonable; without justification for such activities, they were not convinced that the work was necessary. Further, they said that the guidance could have been less standard, tailored instead to meet the needs of different host country cultures and environments, as discussed in Principle VI below.

Embassy officials further suggested that, given their firsthand knowledge of host country environments, they should have been allowed to weigh-in on the Y2K management decisions and guidance that Washington provided to them. In a number of instances, posts made their own determinations regarding what elements of headquarters Y2K guidance to follow. For example, some decided against stockpiling what they considered to be excessive amounts of cash, food, or fuel, given that their host country environments were stable and not very vulnerable to Y2K-related failures. Others used their discretion in remediating and testing systems that did not seem to them to be date-sensitive. Some embassies also decided that they, not Washington headquarters, knew best how to handle emergency situations or evacuations. As one official said, "Y2K demonstrated for the posts that it depends on where you are whether or not you adhere to headquarters guidelines."

Figure 4: Photograph of Cash Reserves at U.S. Embassy Jakarta

Source: State Magazine, February-March 2000.

Eliminate Redundant and Burdensome Reporting Requirements

Host government and industry officials did not understand our inability in the United States to share the same information among ourselves.

— **A Foreign Service Officer**, U.S. Embassy Singapore

Embassy staff that we interviewed indicated that central coordination of data calls from the United States could have made their international Y2K monitoring activities less redundant and burdensome—especially during the last few months before the rollover. For example, embassy staff told us about completing 30-page web reports and answering 83 questionnaires from different agencies and bureaus on similar issues. As the focal point for the U.S. presence in foreign countries, embassies and consulates received data requests from a range of Department of State channels, including Information Resource Management, Chief Information Officer, Diplomatic Security, and Y2K Project Management Offices. They also got requests from other Federal departments and agencies, the Congress, and the President's Council on Year 2000 Conversion.

Embassy staff we met with recognized the need that individual agencies and organizations had for the international Y2K status information, but did not understand why the Federal community could not share the data. Embassy officials observed that the process would have been more manageable if there had been a centralized structure in Washington to filter and coordinate data requests. One Y2K team member cited the IY2KCC web page as a good single source for displaying U.S. information and questioned why the United States lacked a similar center for coordinating the many requests sent overseas. Embassy staff stressed that they could have also benefited from prioritization of the requests, which would have enabled them to appropriately allocate their time. They said that a system to track, monitor, and coordinate requests and consistent feedback from Washington on data received would have also been useful.

Department of State headquarters officials acknowledged that coordinating requests for Y2K information had been a problem and that redundant requests for information may have created a burden for the posts. Gathering such information, however, was key to preserving diplomatic relations and the U.S. presence overseas. Numerous efforts were made to coordinate the data collection requests. For example, the International Interagency Y2K Working Group repeatedly attempted to assign specific areas of interest to individual Federal agencies for collection of information. Similarly, the Bureau for Management sought to minimize taskings of the various Department of State bureaus. In turn, bureau officials said that they tried within their own offices to simplify reporting procedures and minimize the volume of requests to the field, but with limited success. Y2K Project Management Office officials said that in response to embassy concerns, they also took action to reduce the number of questionnaires sent overseas. Despite requirements to coordinate requests through the Project Management Office, we were told that this objective was not fully achieved.

Headquarters officials further indicated that despite the need for improved coordination of requests, at no time did they ask for information above and beyond what could have been provided from sound management practices already in place. They said that information on asset management, contingency planning, and disaster planning should have been readily available from data maintained at post, even before the Y2K problem became a priority.

Consolidate Data Collection Activities Overseas

The United States did not manage the data collection process well. The information from individual countries is important, but our channels for getting it were not in sync.

— **A senior official**, Office of Science and Technology Policy, U.S. Department of Energy

U.S. embassy and consulate officials told us that Federal agency representatives could have better focused their approach to gathering information on Y2K management activities in the various host country environments. Though the Department of State is the focal point for the U.S. diplomatic presence abroad, Foreign Service officials were not the only U.S. officials responsible for collecting international Y2K data. Rather, other agency representatives assigned overseas, as well as visiting delegations by organizations such as OIG, the Department of Defense, the Congress, and consulting firms, also worked to monitor the international Y2K situation. Host country officials, who were repeatedly visited or queried for the same or similar information, were often frustrated by the apparent duplication of effort.

Some Federal officials contended that the Department of State could have better served as the central coordinator or the single collection point for host country Y2K status data. They further suggested that the responsibility for data collection might have been specifically assigned to U.S. embassy economics officers who were generally best positioned to get the Y2K readiness information needed. These officers could have been trained and assigned on a priority, full-time basis to coordinate Y2K monitoring for all of their Federal agency counterparts represented overseas. Other officials countered that the U.S. did not have the right structure—the resources or the people with the right focus—in place to gather international Y2K information. They suggested that a consistent cross-agency team approach, bringing together the information requirements and representatives of the various U.S. agencies overseas, would have been even more appropriate.

Some embassies and Federal organizations did implement effective cross-agency approaches to Y2K monitoring. For example, Department of Defense teams responsible for monitoring Y2K progress in about a dozen countries critical to U.S. security interests abroad included participation by several other Federal agencies, such as the Departments of Energy and Commerce and the U.S. Coast Guard. As discussed in the case study at the end of this section, this Defense approach yielded positive results. U.S. officials suggested that similar strategies could have been used on a more consistent basis to gather Y2K data worldwide. They contended that bringing U.S. embassy and consulate officials that knew the host country environments together with Defense officials that knew the military picture, could have resulted in people talking

jointly with local government and industry to meet everyone's information requirements. Officials also said that there must be recognition that the kinds of information needed for policy-making onY2K often rested in the business environment. Companies overseas were often the best source for this information and, to the extent possible, will need to be included by the U.S. government in future global assessment efforts.

Headquarters officials indicated that overseas data collection and reporting approaches should have followed the pattern set by the centralized headquarters guidance sent to the field. Specifically, the Chief Information Officer informed us that the contingency planning toolkit was specifically designed as direction for all embassy and consulate staff—the entire country team—and not just Department of State representatives. This official indicated that chiefs of mission were responsible for creating a single contingency, disaster, and "day one" plan, which could have served every agency represented at each mission. This single document could then have been sent to each agency headquarters and the Department of State could have spoken with a single voice for the entire foreign affairs community. The Chief Information Officer agreed that the overseas community did receive similar requests from various foreign affairs oversight entities, but asserted that had best practices been followed, each request could have been answered with the same common response. The Washington headquarters perception was that it was not getting adequate responses to their requests, necessitating numerous inquiries to gather the information needed.

Synthesize Analysis of Data Collected

The challenge for the future is to know when to believe the official reports instead of the stereotypes.

— **Chair**, President's Council on Year 2000 Conversion, United States

Obtaining accurate information on the Y2K situation overseas was a major challenge for the United States. International Y2K management activities sometimes were not visible to U.S. observers due to language barriers and a lack of foreign disclosure. Further, as soon as information was obtained, it was often already outdated because the issue was moving so quickly. For a long time, it seemed like a number of countries were not doing much to prepare for Y2K. Consequently, some U.S. analysts and journalists reported whatever information was available and made projections on that basis as to what would happen at the Y2K rollover in a given country. For example, as discussed in the case study to Principle VI below, the United States was concerned that Italy was not preparing for Y2K and would not successfully make it through the transition. U.S. sources had similar concerns about the readiness of Russian gas and nuclear power plants and operations in some newly independent states in Eastern Europe.

Confusion arose when, near the end of 1999, country after country issued reports stating that they were Y2K-ready, contrary to U.S. assessments—including some from our office—that were less optimistic. According to experts that we interviewed, U.S. analysts tended to overlook this self-reported country information in favor of rumors and speculations. In the aftermath of

the Y2K transition, however, it became clear that the people running the foreign systems and governments actually did know best and open source information on their activities should have been trusted. As UN officials concluded: "Y2K status reports from U.S. sources did not always match with that of other countries because the United States tended to always err on the side of more negativity."

U.S. embassy teams reported that their country assessments, often in line with host government reports, were repeatedly second-guessed or met with suspicion. For example, Embassy Rome officials told us that they provided "extensive analysis and input to Washington, but seemed to be reporting into a void on Y2K." Officials at Embassy Cairo were equally frustrated with their reporting efforts. Although they provided details to Department of State headquarters on the Y2K status in Cairo, open testimony on Capitol Hill by the intelligence community countering that Cairo was "collapsing" tended to carry more weight. This caused tense relations between U.S. Embassy and Egyptian officials and created panic among Embassy staff and families. One Embassy official stated that second-guessing must be controlled at some point and the "people on the ground" have to be trusted.

Coordinate Monitoring and Communications Activities

Most organizations set up a command center structure to review status on a regular basis with clear communications flowing in and out. This use of the command center will drive other large systems implementations in the future.

— **Year 2000 Program Director**, a financial institution, London, England

During the Y2K transition, organizations throughout the world coordinated their monitoring and communications activities using a central command and control center model. Such monitoring and coordination centers proved effective in overseeing the Year 2000 date change in nations worldwide. As the date rolled over, technical support staff stood ready and telephone call centers were online. News and press members were also available to report on local efforts, as well as to provide reports on Y2K outcomes in foreign countries that had experienced the date change in earlier time zones.

Several international monitoring systems were cited as invaluable for monitoring the date change. For example, the IY2KCC established the Global Status Watch, a secure web site with standard templates for national governments to use to report their Y2K situations to the public. While such a function was not part of the IY2KCC's original charter or plans, as 1999 progressed it became evident that such a mechanism was needed. Accordingly, national coordinators agreed at the June 1999 United Nations meeting on Y2K to establish such a monitoring facility. According to the IY2KCC, the site was used on a 24-hour a day basis for 8 days during the rollover period, providing sector status information on 159 countries representing 95 percent of the world's population. IY2KCC also developed a color-coded status report to summarize

the extent to which countries worldwide experienced Y2K-related disruptions at the rollover.

Further, the Weathervane Reporting System developed by the Department of State's Y2K Program Management Office provided each embassy's assessment of host nation Y2K status during the millennium transition. The Weathervane Reporting System was a web-based tool used to collect, aggregate, and disseminate status information on critical Y2K rollover dates from over 160 locations. The system allowed all overseas posts, according to a pre-determined schedule, to input Y2K status data to the Department of State Intranet during the rollover period. The information became immediately available within the Department and to the Federal community. U.S. Pacific Command officials, who had established their own Virtual Information Center, stated that they found the Weathervane system very useful. They initially had problems accessing the Weathervane System due to a need for authorization. These officials also had difficulty learning to use the system and experienced limited visibility when they attempted to access certain fields. These are all issues that can be considered and addressed by the Department of State to support future global status monitoring activities.

National and organizational systems and facilities were also developed for monitoring the Y2K rollover. For example, the U.S. established an Information Coordination Center, which served as the Federal point of contact for identifying incidents and coordinating information provided during the Year 2000 transition by national emergency operations centers and the private sector. The Department of State established its own Information Center to centrally collect Y2K reports from embassy teams on the status of their internal operations and host country sectors during the rollover. Like the Global Status Watch and other Y2K monitoring facilities, the Information Center used these reports to produce a color-coded international Y2K status display. The Information Center is depicted in **Figure 5** below.

A number of the monitoring systems and facilities developed for Y2K are now being used for other observation purposes. For example, Mexican officials told us about a monitoring system developed by a national petroleum company. This is still used by managers to monitor current applications real-time. Also, a financial official described an observation system developed for one of its banking offices located overseas, which provided global Y2K wellness checks every 4 hours. While the banking office initially developed this command and control structure for the conversion to the euro currency, it also proved successful during the Year 2000 date change. Further, in addition to the Weathervane Reporting System, the Department of State's Chief Information Officer Organization deployed a comprehensive, web-based system to aid the Computer Incident Response Team in its responsibility for tracking and reporting on cyber terrorist and virus attacks on the Department's domestic and overseas operations. The information that this Computer Incident Reporting System provided was vital to monitoring and ensuring computer security during the Y2K transition. The Department still uses this system today as a tool to determine the security posture of its local area network.

Make Proactive Use of Audit Organizations

The most unsatisfactory [audit] products are those which are based on low priorities in the agency. The [audit organization] should figure out where management is trying to go organizationally and managerially—find out its strengths and weaknesses—and determine how they can support and help drive the [organization] in the direction in which it needs to go.

— **Chair**, President's Council on Year 2000 Conversion, United States

For many in the audit community, the Y2K experience provided an important opportunity for them to work in different and effective ways with their management organizations. Officials around the globe identified audit groups such as the Department of State's OIG, the United Kingdom's National Audit Office, and South Africa's Auditor General's Office as adding value to Y2K management efforts. Managers and audit officials alike have expressed the desire to continue to build such effective working relationships.

For example, OIG visits, begun in mid-1998 to inquire about international Y2K readiness, helped provide a reality check and stimulate remediation progress in a number of countries. Similarly, officials in the Auditor General's Office in South Africa told us that their April 1998 report to the South African Parliament on Y2K issues was their first report ever to get the full attention of the legislative organization. Audit officials also stated that some sector organizations did not even realize that Y2K was a potential problem until the Auditor General's Office contacted them to determine whether or not they had tested their equipment for Y2K compliance. In addition to promoting Y2K awareness to get government agencies and sectors to begin remediating their systems, audit officials believed that they had an ongoing responsibility to monitor Y2K readiness activities, evaluate integrated Y2K testing, and encourage contingency planning.

Figure 5: Photograph of the Department of State Operations Center

Source: State Magazine, November 1999.

Further, the United Kingdom's National Audit Office, which evaluates the operations of principal departments and agencies in the British government, took a novel approach to Y2K management. For the first time, the Office assumed a broader role in analyzing the issue, predicting the outcome, and managing the potential risks. In addition, the National Audit Office worked with Action 2000, the organization responsible for coordinating the United Kingdom's Y2K efforts. One benefit from the new National Audit Office role was the speed with which reports were cleared—some in less than two weeks. Like OIG, National Audit Office reports also provide case studies of effective Y2K management activities.

Case Study on U.S. Department of Defense Approach to Overseas Y2K Assessments

Successfully addressing the Y2K challenge was a top priority for the U.S. Department of Defense. Defense uses information technology systems to support and execute virtually every aspect of its vital peacekeeping and war fighting missions. Defense also relies on technology in host country infrastructures to help sustain military capabilities and operations in various locations overseas. As such, ensuring the continued proper performance of these technology systems through the Y2K transition was imperative.

Under the leadership of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, and with participation by other U.S. agencies, Defense undertook a major effort to review the Y2K readiness of countries where major U.S. military installations are located overseas. Assessment teams were sent to various locations in Europe, Asia/Pacific, and the Middle East. Team objectives were to identify, understand, monitor, and, as needed, assist host country efforts to manage the critical Y2K transition. Of primary concern to Defense was ensuring sustained host country infrastructure operations in sectors such as energy, telecommunications, water, and transportation.

Defense's unique approach to assessing international Y2K readiness had one team study the Y2K status of foreign government entities and infrastructure providers and a parallel team of military contractors talk with foreign infrastructure users (i.e., hotels and retail stores) to get a reading on public confidence. The teams used two separate lines of inquiry that enabled them to validate and crosscheck their findings. Contractors participating on the teams had long been working in the areas studied and were therefore highly suited to the assessment efforts.

Defense credited its partnership with the Department of State as highly instrumental in getting a number of countries to "open their doors" for the assessments. Department of State officials in charge of the Interagency Y2K Working Group were specifically cited for the support they provided. Representatives and technical specialists from other U.S. Federal agencies, such as the Department of Commerce, the Department of Energy, and the Coast Guard, as well as the International Energy Agency either coordinated with or participated in the team's efforts.

The Defense teams sought to obtain firsthand and well-verified Y2K status information on countries such as Italy, Japan, and Germany. Team members chose not to trust the more controversial reports provided by other U.S. organizations without conducting their own assessments. As a result of their assessments, the teams ultimately did not find any major problems with regard to Y2K readiness in these countries. Team officials stated that if they had believed the more negative reports, Defense might have deployed troops, food, supplies, etc. or pulled military families out of the countries to minimize any potential impact of the Y2K rollover. From a foreign policy standpoint, such actions would have been unfortunate, for they could have disrupted relations with the countries involved or created morale problems for Americans living in those environments.

Principle V: Build Public Awareness and Confidence

Y2K management was driven by public perception. Across the globe, many officials realized that, in addition to systems remediation, testing, contingency planning, and other readiness activities, it was equally important to communicate the progress of their Y2K efforts to the public without instilling fear. In some ways, fear can be an effective tool to push people to action. However, many officials, when faced with rampant exaggerations about potential Y2K failures, affirmed that alarmist reports also cause uncontrollable reactions such as tension and panic. They recounted their efforts—with varying success—to deal with emotional issues, promote awareness, and safeguard the public in the event of Y2K-related failures.

"Trust and confidence are the most valuable assets."

— **Staff Director for Management**, Board of Governors of the Federal Reserve System

Manage Fear

There is more misinformation than real crisis.

— **Staff Director for Management**, Board of Governors of the Federal Reserve System

The issue of fear and public confidence was of great concern to Y2K managers. They realized that public overreaction to the Y2K situation could have caused serious problems. For example, hoarding could have occurred due to supply chain fears. Items such as food, water, medicine, and other goods, feared to be in short supply, could have been stockpiled for the Year 2000 date change. Bank runs, described as "very easy to start and explosive," could have resulted from rumors of insolvency in financial institutions. Bank officials expressed concern about potential public behavior and executed plans to keep panic withdrawals of cash from occurring. In addition, public concerns about air travel, both domestically and internationally, could have caused declines in revenues from tourism.

Y2K served to escalate speculations about the potential impact of issues such as embedded chips, nuclear reactors, and terrorism. For example, potential Y2K-related failures of embedded chips were initially feared to create security problems and contribute to business losses. Many companies spent considerable resources pursuing this issue. They later learned that embedded chip problems were overestimated. Additionally, alarms sounded regarding the possibility of failures at Russian and U.S. nuclear power stations. The Department of State played a critical role as facilitator, initiating talks between Russian and U.S. energy officials. The U.S. Department of Energy, the European Commission, the U.S. Nuclear Regulatory Commission, and others worked together to acquire good information on the nuclear situation. They wanted to know whether there were adequate back-up fuel supplies and contingency plans. They also wanted to determine the degree to which technology at the nuclear reactor sites was Y2K compliant. Further, anxieties about computer hackers and other terrorist activities complicating the situation at the Y2K rollover led to heightened public safety and emergency response measures. Specifically,

computer security procedures were tightened up and Internet sites were established to alert the public on the importance of guarding against cyber-terrorism. Ultimately, the world was fortunate that there was no terrorism or security fall-out from the Y2K transition. Tighter security and greater alert at Department of State facilities and other locations worldwide may have helped deter or guard against such attacks.

Efforts to prevent public panic were met with varying degrees of success. The Department of State's presence was generally viewed as helpful in investigating and suppressing Y2K rumors. However, some host country and embassy officials observed that, in certain instances, the United States was viewed as the primary source of the rumors and subsequent panic reactions. For example, noting alarmist tendencies in U.S. press reports, one host country official attributed panic buying of food staples to Americans from the embassy. An embassy official in that country admitted that "Y2K put a ripple of reality" into the lives of American embassy families, showing them the real face of the environment in which they lived and its vulnerabilities.

Officials that we interviewed generally agreed with the philosophy shared by a British telecommunications official: keep all information in the public domain as much as possible. Providing Y2K readiness information to the public had at least two benefits. First, it served to assist in calming public fears about the impending date change. It also had an added benefit of levying political pressure on recalcitrant officials, frequently pushing them to action. Officials at an investment banking organization in London that helped spearhead Global 2000 noted that completing a Y2K assessment and publishing it on the web were important steps to getting people to act. Such disclosures were often followed by improvements in an organization's Y2K rating on the Global 2000 readiness scale--a periodic report on the levels of Y2K preparedness in various sectors and industries.

Similarly, the International Civil Aviation Organization, initially reluctant to publish any Y2K information, found that public disclosure of data on the readiness of air traffic control centers forced countries to take actions to make their systems compliant. Officials in the United Kingdom told us about the open exchange of information between the media and the Central Information Technology Unit, an organization that monitored the Y2K efforts of British government agencies. The Central Information Technology Unit's Y2K media coordination team consisted of reporters that provided not just press statements, but well-founded information based on government assessments. They used the government assessments to give the public a better understanding of the actions taken to address the Y2K problem. During the date change, the press was present at the government's millennium center. This allowed the media to report on activities firsthand and enabled government officials to receive immediate news on worldwide events as the night progressed. British Y2K officials plan to use this type of press involvement to get the word out about conversion to the "euro" currency by July 2002, as part of an ongoing project for the unification of Europe.

Launch Public Awareness Campaigns

[The Y2K] lesson was that companies must communicate what they are doing, give confidence and explain their situation clearly to gain the trust of their customers.

— **A telecommunications official**, Mexico City

Countries worldwide used a variety of methods to raise public awareness and prevent panic concerning Y2K. Some countries provided detailed information to the public on the actions taken by key agencies across the government in preparation for the millennium transition. They also informed the public about contingency plans that had been developed, issued brochures and other reading materials to educate households on Y2K, and held seminars or meetings to address questions from the public on Y2K efforts and activities. For example, reports on coordination efforts by the National Y2K Committee in Mexico served to diminish public concern and increase confidence because they communicated that all of the sectors were working hard on the issue. Similarly, the Singaporean Government conducted an extensive program to mail updates to all its residents on the Y2K status of public utilities and other sectors.

One outreach campaign was specifically geared to Americans traveling overseas. As part of the campaign, Consular Information Sheets—normally released on an annual basis and updated as needed—were revised to include a new Y2K section. Updates to the reports were posted almost daily between September 1999 and December 1999 on the Bureau of Consular Affairs' web site to keep the public informed with continually changing information about international Y2K readiness. The reports are generally prepared by U.S. embassies and consulates overseas, with review and clearance by country desk officers, the intelligence community, the Bureau of Diplomatic Security, and the Department of Defense. The reports provide vital information on travel safety, visa requirements, medical facilities, embassy locations, and safety/security in foreign countries. Another outreach measure encouraged U.S. embassies to hold town meetings for American citizens residing overseas and work through organizations such as overseas schools or adoption agencies networked worldwide to provide updates on Y2K activities. In addition, press conferences were held and public affairs statements were communicated via web sites or e-mail. This entire public affairs strategy used many different tools to reach out to a very broad audience.

Many countries and organizations focused special attention on making small and medium enterprises aware of the Y2K problem. They provided seminars and issued grants to help such firms prepare for Y2K. For example, a technology supplier in Tokyo worked with representatives from various other private sector companies to provide guidance and assist small companies in developing contingency plans in preparation for Y2K. Similarly, Action 2000, a public/private partnership in the United Kingdom, also worked to conduct research, survey companies, and get the Y2K message out to small and medium-sized businesses.

Institute Public Safeguards

As a cautionary measure, many of the police and officials in Japan were on duty to address any concerns or disruptions.

— **A Foreign Service Officer**, U.S. Embassy Tokyo

Police officers, firefighters, and other emergency service organizations customarily face masses of jubilant and boisterous revelers during the New Year holiday. In December 1999, however, they faced additional crowd control issues because of the celebration of the transition to the new millennium, further complicated by the Y2K threat. As a result, extraordinary numbers of emergency response personnel stood ready around the world and throughout the rollover period to oversee the multitudes of spectators intent on ushering in the Year 2000. Engineers, technicians, business managers, and staff of government and business organizations worldwide were also on duty 24 hours per day, prepared to respond to potential crisis situations resulting from Y2K-related failures. For some countries, Y2K proved to be the first opportunity for emergency service organizations to collaborate among themselves, as well as with other public and private organizations, on how to deal with infrastructure failures. This was a departure from previous practices and procedures that were often reactive and were frequently decided only at the top levels of government.

U.S. embassy staff and other U.S. Federal agencies abroad were prepared with newly coordinated or refined warden systems to keep Americans informed of Y2K outcomes throughout the transition period. They were also ready to implement mobilization plans, evacuation strategies, or humanitarian aid procedures as needed. In many cases, embassies were planning not only for the American citizens living abroad, but also for the hundreds of thousands that might have to transit through their host nations should evacuations become necessary.

Ultimately, no Y2K-related evacuations were necessary. However, if evacuations had occurred, millions of people would have needed basic assistance, such as food, water, and shelter. Department of State officials said that they pointed out this potential problem and led efforts to promote awareness of the need for a coordinated United Nations humanitarian response capability in case of major Y2K-related failures. Under normal circumstances, the United Nations loosely manages multilateral assistance for emergency or humanitarian relief. For Y2K, the UN's Office for Coordination of Humanitarian Affairs developed specific strategies to prepare for the impact of potential infrastructure failures on ongoing relief or humanitarian operations and to ensure that clear procedures were in place should extraordinary efforts be needed to address Y2K-related failures. The first line of technical assistance against Y2K-related disruptions was to be national governments. However, alternative relief strategies were also developed, including a plan whereby countries would engage the assistance of their major trade partners that would likely have economic interests in helping them in the event of widespread Y2K-related disasters.

Figure 6: Y2K Considerations for the General Public

Source: Office of Inspector General

Case Study on Hong Kong's Public Relations Program

The Hong Kong Monetary Authority (HKMA), the government organization responsible for maintaining monetary and banking stability, began its Year 2000 management efforts in 1997. Like financial organizations around the world, HKMA faced uncertainties regarding the ability of national monetary systems to accommodate the Y2K date change. HKMA officials recognized, too, that Y2K was not solely an IT issue, but also an issue of public trust—that it was important for financial institutions to reassure their customers that banking systems would be unaffected by the Y2K transition.

HKMA required banks to take several steps to build confidence and mitigate potential impacts on operations during rollover periods. Beginning in 1998, HKMA had banks disclose information on Y2K efforts in their financial statements. They also required banks to develop awareness programs to allay customer concerns about the millennium bug. Under HKMA direction, over one-half million leaflets on Y2K management activities were sent to bank customers. Among other things, banks also released public interest advertisements, set up dedicated hotlines to answer customer inquiries, and kept up-to-date Y2K status information posted to their web sites to support the Y2K transition.

HKMA commissioned consultants to conduct a series of public opinion surveys on the Year 2000 issue. The surveys, held between May 1999 and January 2000, had over 1,000 respondents. The survey results enabled HKMA to better measure and track public concern and to refine, if needed, its communications strategy. The results remained confidential until after the Y2K transition to avoid arousing unnecessary anxiety or speculation. Generally, the number of respondents knowledgeable about Y2K remained low. Those that were aware, however, expressed a high degree of confidence in the banking sector's ability to address the challenge.

As a part of its Y2K contingency planning efforts, HKMA established an Event Management Center. Its threefold purpose was to monitor the performance of monetary and banking sectors in Hong Kong and overseas, to communicate with the media and local and overseas markets, and to coordinate emergency responses during key date changes. The Center operated around the clock during critical periods in September and December 1999, and in February 2000, receiving Y2K performance reports from authorized institutions, payment systems, and major infrastructure providers.

The greatest boost to public confidence came from the September 9, 1999, rollover test. While most Y2K experts viewed this date as a nonissue, HKMA did not downplay its significance. HKMA used this opportunity to cultivate public and media interest. Successfully passing the September 9, 1999, rollover tests greatly diffused public concern. Once people saw the outcomes, precautions to bolster public confidence became much less necessary. After months of preparation, Hong Kong's financial sector entered the Year 2000 without major disruptions. Hong Kong opened for business on January 3, one of the world's first financial centers to launch operations in the New Year.

Principle VI: Consider Cultural Differences

Consideration of national, cultural, and environmental differences should be a natural aspect of any global management program. Such consideration is needed to ensure that management strategies are appropriately applied and that progress and activities toward meeting objectives are accurately assessed in the context of the many different countries worldwide. In Y2K management, however, expectations from some industrialized nations—particularly the United States—as to when and how other countries would prepare their systems and infrastructures for the millennium rollover were often based on strictly Western perspectives and approaches. Some organizations in this country did not adequately factor into their international Y2K monitoring approaches several inherent differences among nations regarding their levels of IT complexity and dependence, need for oversight, views of crisis management, or approaches to information disclosure. U.S. lack of appreciation for these differences resulted in international misunderstandings, disagreements, and sensitivities that we should avoid in undertaking multilateral challenges in the future.

"The countries ahead in Y2K resolution made a terrible mistake. The approach that they adopted was the same everywhere and this was not correct."

— **National Y2K Coordinator**, Rome, Italy

Look Beyond Western Perspectives and Approaches

The underlying assumption of these Western approaches was that if a country did not look like us, then they were failing. This was not true. All it took to find the truth was to talk to people.

— **A senior official**, Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence, U.S. Department of Defense

A major lesson learned from the Y2K exercise is the need to think more broadly in undertaking international projects and recognize that foreign countries do not necessarily manage or react to issues in the same manner that we do. However, officials told us that in promoting and monitoring international readiness for the millennium rollover, some U.S. organizations tended to view foreign Y2K programs from their own Western perspectives, holding flawed expectations as to what overseas time frames and strategies for achieving Y2K readiness should be. Such U.S. monitoring efforts did not adequately consider differences among worldwide cultures, infrastructures, and perspectives that predetermined foreign countries' individual requirements and programs for managing the Y2K problem.

In keeping with their Western perceptions and expectations, we were told that some U.S. organizations also tended to use template data collection approaches to assess international Y2K readiness. Assuming that all countries were alike in facing Y2K, they weighed and analyzed the information compiled in like manner from country-to-country. Such uniform monitoring

approaches did not incorporate more tailored assessment questions or more qualitative research that would have helped get at the truth about the progress of a particular country's Y2K programs. Too often, the analyses lacked firsthand data from the countries in question, unlike the dual-tracked approach taken by Department of Defense teams, as discussed in the case study for Principle IV above. By the time such analyses were completed and the assessments publicized, the information was often outdated and inaccurate.

The following are several international distinctions that officials believe U.S. organizations should consider to improve their approaches to managing global IT issues in the future.

- **Different levels of IT complexity:** The United States is a sprawling nation with a preponderance of highly distributed, wide-ranging, heavily integrated, and often "leading edge" technology. As such, Y2K posed a highly complicated challenge for American business and government managers. While other industrialized countries were often confronted with many of the same issues and used the same basic readiness approach as the United States, their Y2K problems often did not achieve the same levels of complexity as those of the United States. For example, centralized sector operations or partial government ownership of utilities and companies in countries such as Singapore or Mexico made it easier to issue and enforce Y2K management direction. Predominant reliance on standard or off-the-shelf technology as opposed to wide-ranging custom-built systems in some governments made remediation activities relatively straightforward. And the fact that economies such as Italy are reportedly predominantly comprised of many small private companies that are not heavily automated made Y2K readiness relatively less burdensome.

- **Different levels of IT dependence:** Many parts of the world have been slower to automate than the United States. Countries worldwide—especially developing countries—still rely on manual, mechanical, or paper-based processes. In many locations, technology is sparse and sometimes so old that it was not date-sensitive and thus not vulnerable to Y2K. Significantly lower levels of IT dependence made Y2K preparation in many nations less extensive and much easier to deal with than in the United States. For example, officials in Chile told us that their water distribution systems are gravity-fed and manually operated, railroad systems are not digitized, and reliance on electricity in homes is relatively less than in the United States due to the availability of other energy alternatives such as gas or coal. A Foreign Service official formerly assigned to Bangladesh said that the infrastructure in the country was so old, or imported equipment was so new, that Y2K was virtually a nonissue. Oil refineries in some parts of Mexico are manually run. Banking in places such as Macau is not centrally controlled and many other operations are not even computerized. And water management operations in Egypt are almost totally mechanized, but separate from wastewater management, which is becoming automated but remains a simplistic, nonintegrated process.

- **Unequal need for U.S. oversight of worldwide management activities:** Because all countries worldwide did not face equal Y2K threats, they also did not necessarily need equal U.S. oversight of their Y2K activities. Officials charged with U.S. oversight responsibilities found that attempting to monitor Y2K to the same degree in every nation was a waste of time. Officials suggested that the nations that were likely at most risk of Y2K disasters were the ones in the middle that lacked technical expertise, but had just enough IT dependence to make them vulnerable. For example, Eastern European nations on the verge of becoming "first world" might be included in this group. They suggested that the United States should have been less concerned than they were with monitoring "high-tech" locations—sending teams out to repeatedly ask embarrassing readiness questions of nations like England or Singapore that were already on top of the Y2K situation. Additionally, though the United States did well to provide Y2K guidance and support, we also should have been less concerned with Y2K oversight in developing nations that have relatively little automation to remediate or critical infrastructure to protect.

- **Different foreign strategies to meet the deadline:** Too often in Y2K monitoring, Americans prematurely decided that other nations of the world—particularly developing nations—would not be ready in time for Y2K. U.S. organizations expected other nations to work on the same timetable and to use the same strategies that we did in managing Y2K. Seeming delays, lack of concern, or alternative approaches in addressing Y2K by countries such as Italy or Mexico worried us. We did not anticipate the amount of "last minute" remediation and emergency preparation that these nations would accomplish in the final months of 1999. We were taken by surprise by these countries' ability to build on the knowledge and successes of forerunners in Y2K management—adapting the tools, methodologies, and strategies that they provided—and "leap-frog" ahead to meet the Y2K deadline. Nor did we foresee the ability that developing countries exhibited to easily revert to manual processes, institute stopgap measures, or reset computer clocks to earlier dates to ensure minimal operational disruptions during the millennium transition.

- **Different world views of emergency preparedness**: According to some Y2K officials, the United States assumed that the rest of world shared our view of emergency management. We also thought that they all saw the Y2K situation as a crisis issue that they would have great difficulty overcoming. This country did not appreciate that, because of the vulnerabilities, disruptions, and disasters that they periodically face, many countries have tremendous ability to cope with crises—in some instances, even better than the United States itself. Outages, breakdowns, and natural disasters are common to many countries of the world. For example, officials in Chile said that portions of the country are used to power outages. Further, other countries such as Mexico and Nepal are at high risk of experiencing earthquakes. Any Y2K-related disruptions, some thought, could not be much worse.

Given their different experiences and environments, foreign countries were generally less given to stockpiling of goods and supplies and panic preparation for Y2K than the United States. By design, some nations tended to delay readiness or did not do much at all to manage the problem in advance. Other places such as Hong Kong or Japan had long been in the disaster-planning mode, while places such as Chile already had built-in backup via alternative energy supplies. Still other nations hesitated to take any action at all to counter the threat due to cultural or traditional beliefs. In general, foreign nations worked to downplay the situation and avoid the alarmist tendencies imported from the United States or other industrialized nations.

- **Divergent foreign perceptions regarding information disclosure**: The United States and other Western nations are information disclosure-oriented. Official information, both good and bad, is routinely shared with the public and is often backed up with official briefings and candid press releases. In preparing for Y2K, the United States expected similar information disclosure, trust, and sharing by foreign industries and governments. When countries did not openly publicize their Y2K activities, Americans took that to mean that they were not doing anything. In truth, however, parts of the world were simply reluctant to openly share official information. Some such as Egypt considered it sensitive and detrimental to the wellbeing of their national economies. Recognizing that company privacy is strong and needs to be protected, other governments such as Italy resorted to low profile approaches to oblige companies and administrative bodies to provide information on their Y2K readiness efforts.

  Further, some countries did not recognize the importance of reporting in English on their Y2K programs so that their progress and activities would be readily discernible to the outside world. To the United States, the lack of English language documents on Y2K indicated a lack of remediation effort, but this was not necessarily true. For example, in 1998, lacking the information and documentation to indicate otherwise, many U.S. observers became concerned that the Japanese had started managing the problem too late and would not be done in time. Once Japanese officials learned that the lack of English-language publications conveyed a message that they were delinquent in Y2K remediation, the country moved to becoming more transparent. Similarly, at one point there was some international concern about the Y2K readiness of a Russian natural gas producer on which many neighboring countries depended for supplies. There was little independent, English-language information available to confirm the gas producer's readiness assertions. According to IY2KCC reports, the concern was not dispelled until a gas company in Finland posted in English the results of its own assessments and inspections of the gas producer's readiness on the web.

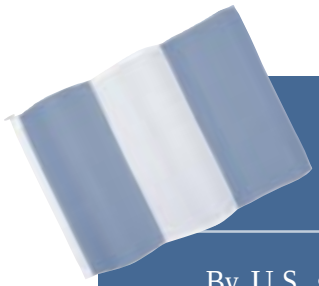
Avoid Misinterpretations of Foreign Approaches

The United States was looking at the Y2K problem from a Western world perspective and therefore didn't believe the…reports where countries self-reported that they would be okay.

— **A management consultant**, Santiago, Chile

Officials worldwide told us that, as a result of Western perceptions and template assessment approaches, a number of U.S. organizations got their international Y2K assessments wrong. Based on misinterpretations of information provided from the field, private and Federal organizations released reports that foreign countries were failing or falling behind in Y2K readiness activities, even though field reports and subsequent outcomes disproved these allegations. Officials said that too often, these organizations assumed that if countries were not taking the U.S. approach to Y2K, then they were doing it wrong. Blinded by preconceived ideas as to the progress that foreign countries should have been making in managing Y2K, several U.S. organizations also tended to not believe self-reported information from the countries themselves that their Y2K management efforts were on target. U.S. organizations did not foresee that despite, or sometimes because of their differences, foreign countries would ultimately be just as successful as the Western world in managing or averting a Y2K crisis in their individual country environments.

In a few instances, U.S. reports on the status of international Y2K readiness efforts had negative impacts on U.S. embassy and host government relations. For example, this was true in the case of Japan where, as cited above, the country's failure to publish information on its Y2K program in English led to negative impressions that they were late in addressing the problem. As a result of the misunderstanding, some Japanese and U.S. embassy officials were sensitive on the issue of information disclosure when we met with them to discuss it. Further, after some embarrassing interim reports from the United States on Egypt's Y2K progress, U.S. embassy officials classified the information they reported on the country's Y2K readiness in order to regain the trust and confidence of country officials with whom they routinely dealt. The following case study on U.S. assessments of Y2K progress in Italy further demonstrates how Western misperceptions impacted U.S. Embassy/host government relations.



Case Study on U.S. Assessments of Italy's Y2K Readiness Program

By U.S. standards, Italy was late in starting Y2K remediation. The country in general did not seem to view Y2K as a big issue and spent less time on it than many other nations. Due to a lack of funding, the Italian National Y2K Committee was not established until December 1998, although the government had mandated its formation six months earlier. There were also few publications and a lagging response to U.S. inquiries about Italian Y2K activities and progress.

American analysts and journalists made much ado about Italy's seeming lack of concern about Y2K. They issued highly pessimistic reports that the country was doing nothing to address the problem. A December 1999 news article also lampooned Italy for its lack of Y2K progress and anticipated that the nation would have difficulty making it through the rollover period. U.S. Embassy officials generally found nothing through open source information or their monitoring efforts to indicate serious problems with ItalianY2K readiness. They said, however, that their reports to Department of State headquarters in this regard were reduced to standard terminology that was insufficient to balance the negative perceptions already in existence. Embassy officials' concerns about headquarters treatment of the information they presented were disregarded.

Italians did not understand why officials in the United States did not believe reports that they were addressing Y2K. Although they were working on a different timetable than the United States, many Italians were confident that their Y2K program would turn out fine. They benefited from cooperation with the European Community and other forerunners in Y2K readiness, extracting from them a blend of information and practices—management guidelines, organization structures, methodologies, automated tools, contingency planning approaches—that enabled them to "leap-frog" ahead in progress. The fact that many companies in Italy are not highly automated also helped. Companies that relied on technology had long been working on Y2K and were well prepared. For example, financial institutions, working in conjunction with Global 2000 and the Central Bank of Italy, were the first in Italy to begin addressing the problem. Italians did not widely publicize their Y2K efforts due to lingering uncertainties about the final outcome and a belief that too much disclosure in the interim would create public panic. They indicated, however, that U.S. Embassy officials and representatives of U.S. agencies who visited Italy readily discerned the Y2K progress being made under the surface.

Italy was vindicated in its Y2K approach when they made it through the millennium transition period with minimal disruptions and no major impact. The press made efforts to recoup its earlier lampoon shortly after the New Year, with an article stating that Italy performed well in managing Y2K after all. However, the damage had already been done. According to U.S. Embassy officials in Rome, U.S. conduct in the assessments was viewed as heavy-handed and undiplomatic.

Opportunities for Applying Successful Global Project Management Practices

Although Y2K is over, there are nonetheless a number of specific management activities which, begun under or derived from the past few years' global management exercise, continue to live on. Organizations in different locations across the globe described such activities as Y2K legacies from which they individually, regionally, or globally continue to benefit. Some of the activities are ongoing; others are in the initial stages of implementation. Like our case studies, the activities demonstrate in actual application some of the effective principles and practices of Y2K management, as discussed above. Several of the Y2K carryover activities that officials shared with us are highlighted below.

UN Registry of IT Focal Points:

As mentioned in the case study to Principle I above, the Chair of the United Nation's Working Group on Informatics built the initial registry of about 400 Y2K points of contact in nations worldwide. Run on the UN Development Program server in New York, the registry constituted a secure network for working group members and points of contact to use to send messages and share information on Y2K problems and what could be done to address them. Following Y2K's success, with the belief that it would be unwise to let the network disappear, it was decided to maintain the network and expand its use to other issues. UN officials subsequently sent out an e-mail to all on the list, requesting updated information on national IT focal points and their alternates who could deal with broader IT issues, not just Y2K. The network is currently available to provide information on and access to IT contacts in 188 countries worldwide. The network has already been used to survey individual nations on such issues as the legislation they have in place regarding the Internet and the extent to which they are ready for e-commerce. UN officials expect that the network will have additional uses in the future.

South American Coordination:

According to internal auditing officials for the Government of Chile, entities and individuals in South America that worked on Y2K are trying not to forget the past few years of cooperation and intense teamwork. Though Y2K has ended, they have an interest in continuing to work together and are using the networks established through the Y2K project to keep in touch. Government audit officials are evaluating and developing a report on regional Y2K management activities as a model for continuing cooperation. They plan to hold a conference to determine how best to use the networks and methodologies established under Y2K as a means for increasing technology development and addressing other government modernization and humanitarian issues.

Project Management Approaches:

A number of officials told us that they are applying the processes and methodologies developed under Y2K to managing other large projects in their organizations. For example, banking officials in London are using the Y2K-developed strategies to help manage a project to convert to the euro currency by 2002. Banking officials explained that, similar to Y2K management, the project involves systems inventories, massive systems conversions, evaluation of business impact, end-to-end testing, contingency planning, command center monitoring and control, constant communications, and building public awareness. Also like Y2K management, the bank project is managed by IT and business representatives working together. The bank now has a global governance model based in Europe, with steering committees worldwide.

> "The international cooperation regarding Y2K was not just wishful thinking, but reality. There are other issues on which the world needs to work together."
>
> — **Ambassador**, Permanent Mission of the Kingdom of Lesotho to the United Nations

Further, telecommunications officials in London are applying Y2K project management methodologies to a human resources management transformation program. Currently human resources management at this company requires excessive paperwork and manpower. The new program would make all human resources management policies and procedures accessible to business managers at the desktop. Managers would only have to interface with human resources specialists when the issues encountered are too complex for them to handle. The program will require new applications and web interfaces and is expected to result in massive reductions in personnel costs.

Contingency Planning and Crisis Management:

In preparation for Y2K, UN officials developed contingency and evacuation plans for their operations in New York City. A recommendation has been presented to UN senior management to support continual update of the plans, despite scarce resources and the absence of a Y2K-like threat. Similarly, officials at the U.S. Embassy in Mexico City recommended that the crisis center that they established in the embassy under Y2K readiness be maintained to help them manage in case of other emergency or natural disaster situations. The center includes back-up communications and crisis management procedures that could be implemented at a moment's notice.

Technology Systems and Tools:

Organizations are making innovative use of IT to help continue the international sharing and communications begun under Y2K readiness. For example, the U.S. Pacific Command is currently implementing a password-protected, Internet-based network to enhance political/military cooperation and encourage communications and sharing of open source information in the Asia Pacific region. Further, like the free, multilingual compact disk distributed to promote Y2K readiness overseas, Commerce officials are developing another tool to help international managers plan their IT investments. Officials plan to prototype, test, and ultimately distribute this product overseas via technical seminars patterned after their Y2K workshops. The plan is to get host countries and U.S. suppliers on board early to support this effort, because the financial resources needed are no longer available like they were during preparations for Y2K.

Aviation Frequency Protection:

U.S. Federal Aviation Administration officials told us that for years, they lobbied to protect aviation frequency from cellular phone companies that seek to gain greater portions of the frequency spectrum. As a result of the cooperation begun under Y2K, aviation organizations have now joined together to counter the incursion. If the cellular phone companies had been successful, they could have hurt advances in "free flight"—a new system of air traffic management that the Federal Aviation Administration is trying to promote. Free flight will provide controllers and pilots with new technologies and procedures that will allow them to increase the safety, capacity, and efficiency of air traffic operations.

As we have suggested, and as officials worldwide have agreed, the effective practices and lessons learned from Y2K management may be beneficial in helping address still other global IT issues as we move forward in the new millennium. For example, officials that we interviewed surmised that critical infrastructure protection is likely the next major issue with which the world will have to contend, due to the importance of IT to national and international processes and operations in just about every sector imaginable. They reflected that Y2K risk assessments and contingency planning were actually first steps in addressing this issue. Additional steps include putting in place the policies and procedures needed to guard against physical and online attacks and other operational disruptions on a continuing basis. As the Italian National Y2K Coordinator indicated: "Y2K was an alarm. Security is the main issue and point to address."

Officials suggested that the increasing spread and reliance on computer technology around the globe makes it all the more likely that another global IT management crisis will occur in the next two decades. The warning signs are evident:

- On May 4, 2000, the so-called "I Love You" virus created computer chaos around the world, possibly costing business and government organizations billions of dollars.
- Some experts have suggested that the Internet may soon run out of addresses using current protocols, prompting a need to change how computer systems recognize and process such addresses.
- Telecommunications experts estimate that the U.S. will run out of telephone numbers within the next 10 to 15 years, requiring strategies to extend the life of the U.S. numbering system and avoid overhaul of the computers that process those numbers.
- The so-called "digital divide" issue, regarding the disparities between nations that have and do not have technology, poses a major issue for those who are striving to promote economic development in the developing world.

Further, officials that we interviewed indicated that effective practices and lessons learned from Y2K management are not limited in their applicability to global IT issues alone. They suggested that Y2K management approaches might also be applied to programs to overcome major international challenges such as terrorism, drought, and global warming. The Y2K experience can also be considered in devising approaches to addressing world health issues such as famine and acquired immune deficiency syndrome, which have reached epidemic proportions in some locations.

There are nonetheless several challenges that must be overcome to manage such issues in similar fashion to what was done under the global Y2K project. The answers on how to overcome these challenges are not entirely clear. For example, the fact remains that there is currently no focus or incentive for undertaking other global projects to address the emerging IT issues identified. According to the Former Chair of the President's Council on Year 2000 Conversion, a formal structure could result in a global IT agenda with a geo-political force behind it. However, despite Y2K's success, there is still no permanent structure in place to deal with global IT issues. The communications and cooperation begun under Y2K were never institutionalized and much of the activity has been discontinued. As discussed in Principle I above, much of the cooperation under Y2K was based on individual leadership efforts—something that could not be institutionalized. An international force could take the initiative to bring nations and sectors together and build trust around addressing IT issues. Once again, leadership from the United States as well as other G8 nations will be vital for any international cooperation effort to succeed.

As discussed in Principles IV and VI, the United States, along with other industrialized nations, will also need to modify future approaches to working with developing nations to address global IT and other shared management issues. It has been suggested that the industrialized nations were too directive under Y2K management. For the future, a process is needed whereby developing nations tell the industrialized world what they need and not vice versa. Such an approach will help counter Western misperceptions and the Y2K problems with data collection, reporting, and analysis, reported above.

Finally, global disaster management remains untested. Since there were reportedly no major problems to deal with as a result of the Y2K transition, if a real global disaster were to occur, we have no idea what the results would be. There is still no evidence of the world being able to handle multiple problems at one time, as we anticipated under the Y2K exercise. There is also no evidence of the global ability to effectively manage the simultaneous movement of people or communities under proposed mass evacuation strategies. But even while there is expectation that planned global crisis management strategies are effective, there is hope, too, that they will never have to be implemented.

Appendix A

Related Products

Best Practices and Lessons Learned, National Y2K Information Coordination Center, June 19, 2000.

Consular Best Practices and Lessons Learned from Y2K, U.S. Department of State, Consular Affairs Memorandum, March 24, 2000.

Coping with Y2K Organizational Adaptation and Change at the U.S. Department of Transportation, U.S. Department of Transportation, Office of Emergency Transportation, Research and Special Programs Administration, June 2000.

Final UNDP Y2K Task Force Report, United Nations Development Programme, January 14, 2000.

*Impact and Lessons Learned (*excerpt from *InfoDev Y2K Initiative Report)*, World Bank, *info*Dev, as of September 18, 2000.

Informe Final Problematica Ano 2000, Petroleos Mexicanos, Mexico City, Mexico, as of September 18, 2000.

Lessons Learned, Briefing Presentation of the Y2K Project Management Office, U.S. Department of State, as of August 2000.

Lessons Learned from Year 2000 Experience, President's Council on Year 2000 Conversion, Financial Sector Group, as of July 27, 2000.

Lessons Learned from the Year 2000 Project, Federal Financial Institutions Examination Council, March 21, 2000.

Lessons Learned, ITU – Telecommunications Standardization Sector, Temporary Document GEN – 36, Study Group 2, Geneva, March 7-17, 2000.

Managing Y2K at United Nations Headquarters: Lessons Learned for Future Complex Emergency Situations, Lessons Learned Unit/ DPKO in cooperation with Management Policy Office/DM, United Nations, August 2000.

Modernising Government in Action: Realising the Benefits of Y2K, Presented to the Parliament by the Rt Hon Margaret Beckett MP, President of the Council and Leader of the House of Commons by Command of Her Majesty, April 2000.

Office of Treasury Reinvention: Year 2000 Lessons Learned, U.S. Customs Service, as of September 11, 2000.

Problema Informatico del Ano 2000 (Y2K), Comision Nacional de Energia, Santiago, Chile, as of April 12, 2000.

Reflections on Global 2000, Tim Shepheard-Walwyn, Global 2000 Coordinating Group, February 17, 2000.

Report on the Computer Year 2000 Problem (Provisional Translation), The Y2K Office of the Cabinet Secretariat, Tokyo, Japan, March 30, 2000

Report to Congressional Defense Committees Year 2000 (Y2K) Lessons Learned, as requested in Report of the Committee on Appropriations on the Department of Defense Appropriations Bill, 2000, Report 106-244, March 15, 2000.

Summary of Y2K Consumer Protection Efforts, Bureau of Consumer Protection, Federal Trade Commission, March 2000.

USCINCPAC Y2K Lessons Learned, United States Commander in Chief, Pacific Command, February 1-2, 2000.

Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges, U.S. General Accounting Office, (GAO/AIMD-00-290, September 2000).

Y2K Aftermath - Crisis Averted Final Committee Report, The United States Senate Special Committee on the Year 2000 Technology Problem, Summary of Committee Findings, February 29, 2000.

Y2K International Project: Lessons for the Future, The MITRE Corporation: McLean, VA, June 28, 2000.

Y2K: Starting the Century Right!, Report of the International Y2K Cooperation Center, Washington, DC, February 2000.

Y2K Support for the Egyptian Electric Authority (EEA) - Final Report, U.S. Agency for International Development (USAID) - Energy and Environment IQC, Task Order No.: 263-224, IQC No.: LAG-1-00-98-00004-00, Reporting Period: August 22, 1998 - January 31, 2000.

Year 2000 Legal Issues and Legislation, Charles V. Dale, Legislative Attorney American Law Division, CRS Report for Congress, Order Code RS20159, Updated January 12, 2000 (Limited Distribution).

Appendix B

Acknowledgements

We would like to acknowledge the following organizations whose advice and assistance throughout this project have been invaluable.

Organizations Visited Domestically

Department of State, Washington, DC

Bureau Certification Strike Force Team

Bureau of Consular Affairs

Bureau of East Asian and Pacific Affairs

Bureau of Western Hemisphere Affairs

Bureau of International Organization Affairs

Bureau of Public Diplomacy and Public Affairs

Chief Information Officer

Contractor for A Logical Modernization Approach (ALMA)

MILVETS, Contract Organization

Office of Special Representative for Y2K International Coordination

Y2K Program Management Office

International Organizations

European Commission
(Visiting Delegate)
Information Society
Directorate-General
Brussels, Belgium

International Monetary Fund
Technology and General Services Department
Washington, DC USA

International Y2K Cooperation Center
Office of the Director
Washington, DC USA

Organization of American States
Information Management Office
and Office of Inspector General
Washington, DC USA

The World Bank
*info*Dev Program
Washington, DC USA

United Nations, New York, NY

Economic and Social Council
Working Group on Informatics

Department of Management and Administration

Information Management Services Branch

Permanent Mission of the Kingdom of Lesotho

United Nations Development Programme, Division for Administration and Information Services

U.S. Mission to the United Nations
Administrative Counselor's Office

United States Federal Organizations

Agency for International Development
Information Management Office
Washington, DC USA

Central Intelligence Agency
Directorate of Intelligence
Langley, VA USA

Coast Guard
Year 2000 Project Team
Washington, DC USA

Department of Commerce
Office of Computers and Business Equipment
Washington, DC USA

Department of Defense
C4I Investment Strategy Division
Washington, DC USA

Office of the Assistant Secretary of Defense
Crystal City, VA USA

Department of Energy
Office of Science and Technology Policy
Washington, DC USA

Department of Transportation
Office of the Deputy Secretary
Washington, DC USA

Federal Aviation Administration
International Office
Washington, DC USA

Federal Reserve Board
Staff Director for Management
Washington, DC USA

President's Council on Year 2000 Conversion
Office of the Chairman
Washington, DC USA

US Pacific Command
Foreign Policy Office
Camp H. M. Smith, Hawaii USA

United States Private Industry

American Express Company
Government Affairs
Washington, DC USA

Citigroup Inc.
Year 2000 Enterprise Project Office
New York, NY USA

Deutsche Bank Securities
Managing Director's Office
New York, NY USA

Mitre
Advanced Intelligence
Systems Office
Economic and Decision
Analysis Center
McLean, VA USA

Science Applications International Corporation
Center for Critical Infrastructure
Protection
McLean, VA USA

Organizations Visited Overseas

Cairo, Egypt

Host Country Contacts

Central Agency for Public Mobilization and Studies

Egyptian Civil Aviation Authority
Air Traffic Services Sector

Government of Egypt
Ministry of Electricity and Energy

Greater Cairo Waste Water Authority

Information and Decision Support Center

Ministry of Petroleum

National Information Center for Health and Population
Director General's Office

US Embassy Contacts

Administrative Counselor Office

United States Agency for International Development

Deputy Chief of Mission

Economic and Political Office

General Services Office

Information Management Office

Office of the Defense Attaché

Regional Medical Office

Regional Security Office

Hong Kong, China

Host Country Contacts

British Consulate General

Cable and Wireless
Hong Kong Telecom

Hong Kong Monetary Authority
Banking Policy Department

Information Technology and Broadcasting Bureau
Secretary's Office

US Consulate Contacts

Administrative Office

Deputy Principal Office

Economic and Political Office

General Services Office

Information Management Office

Regional Security Office

London, England

Host Country Contacts

Barclays Bank
Group Treasury Office

British Telecom
Network British Telecom

Cabinet Office
Central IT Unit

Cable and Wireless, Ltd.
Y2K Team

Citibank
Year 2000 Program Office

International Chamber of Shipping
Secretary General's Office

National Audit Office
Information Technology

UBS Warburg
Europe, Middle East and Africa Office

US Embassy Contacts

Administrative Office

Environmental Science and Technology Office

General Services Office

Information Management Office

Regional Security Office

The Minister

Mexico City, Mexico

Host Country Contacts

Banco de Mexico
Information Systems Office

Luz y Fuerza Del Centro
Technical Services Office

National Commission for the Year 2000 Systems Conversion
National Institute of Statistics, Geography and Information

Petroleos Mexicanos
Information Technology Office

Servicios a la Navegacion en el Espacio Aereo Mexicano
General Technical Office

TELMEX
Quality Assurance Office

US Embassy Contacts

Environmental Science and Technology Office

General Services Office

Information Management Office

Regional Security Office

Rome, Italy

Host Country Contacts

Ente Nazionale Energia Elettrica
Transmissions Division

Ente Nazionale Idrocarburi
Y2K Project Office

National Y2K Coordinator

Telecom Italia

US Embassy Contacts

Consular Affairs

General Services Office

Economic and Political Affairs Office

Financial Management Center

Information Management Office

Public Affairs

U.S. Agency for International Development

Santiago, Chile

Host Country Contacts

Asociacion de Bancos e Instituciones Financieras

Regional Coordinator for South America and President of the Council of Government Internal Auditors

Comision Nacional de Energia
Industrial Civil Engineer Office

Ministerios de Transportes y Telecomunicaciones

Price Waterhouse Coopers

US Embassy Contacts

Facilities Management Office

Information Management Office

Political and Economic Office

Regional Security Office

Singapore

Host Country Contacts

Civil Aviation Authority of Singapore
Information Systems Office

Infocomm Development Authority of Singapore
Government Chief Information Office

Ministry of Health
Information Management Division

Monetary Authority of Singapore
Financial Supervision Group

Public Utilities Board Singapore
Computer Services Division

US Embassy Contacts

Deputy Chief of Mission

Defense Attaché Office

Economic and Political Office

Federal Aviation Administration

Financial Management Office

General Services Office

Information Management Office

Regional Security Office

Tokyo, Japan

Host Country Contacts

Financial Supervisory Agency
International Affairs

Government of Japan
Cabinet Secretariat

International Business Machines
IBM Global Services

Ministry of International Trade and Industry

Ministry of Posts and Telecommunications
International Policy Division

Nippon Telegraph and Telephone Corporation
Information Strategy Planning Section

Sony Corporation
Year 2000 Group

US Embassy Contacts

Administrative Affairs

Consular Affairs

General Services Office

Information Management Office